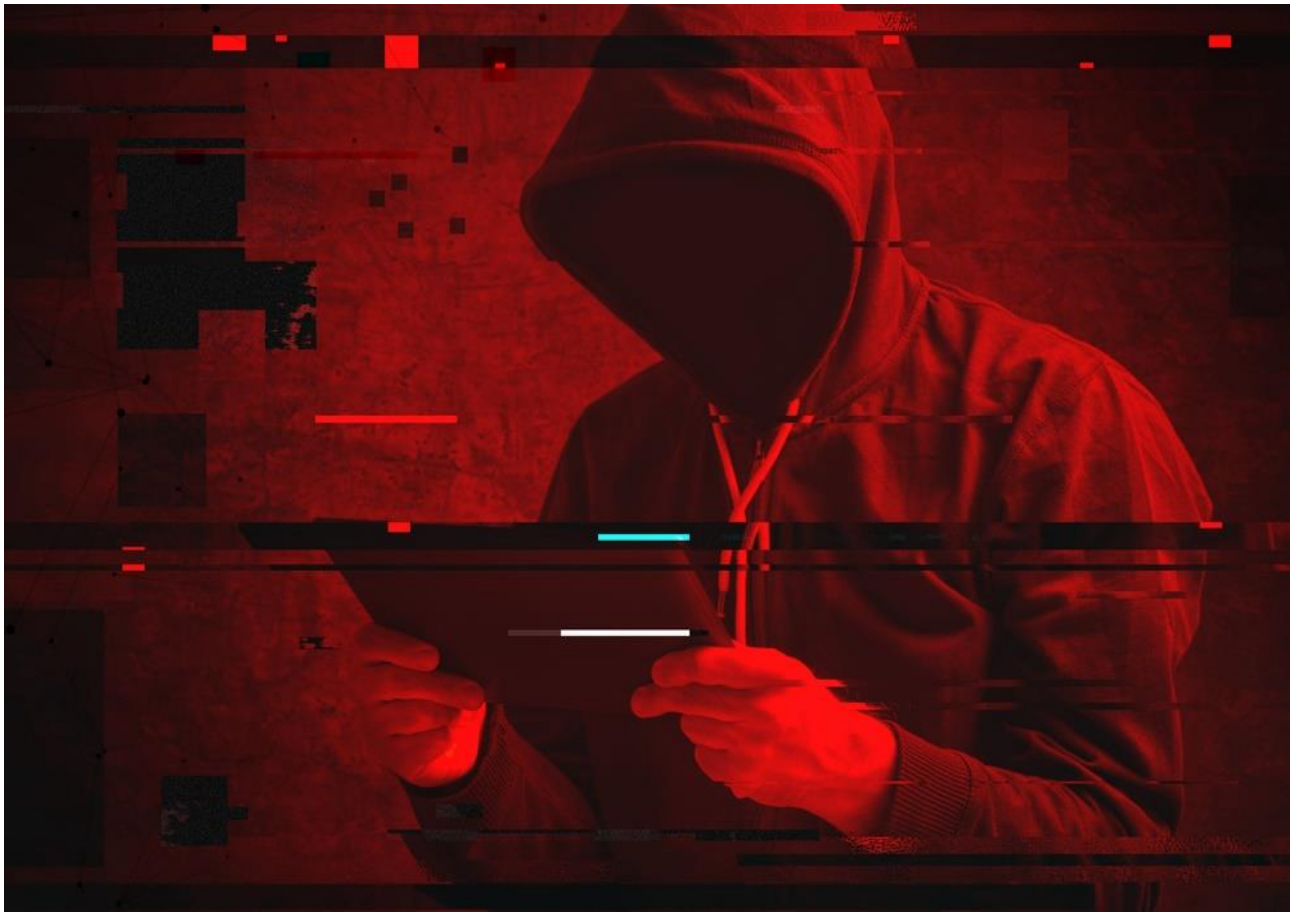


IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud

Michael Spjelkavik Mark, Cathrine Tømte,
Terje Næss og Trude Røsdal

Rapport 2017:32

NIFU

IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud

Michael Spjelkavik Mark, Cathrine Tømte,
Terje Næss og Trude Røsdal

Rapport 2017:32

Rapport 2017:32

Utgitt av Nordisk institutt for studier av innovasjon, forskning og utdanning (NIFU)
Adresse Postboks 2815 Tøyen, 0608 Oslo. Besøksadresse: Økernveien 9, 0653 Oslo.

Prosjektnr. 12820809

Oppdragsgiver Justis- og beredskapsdepartementet
Adresse Gullhaug Torg 4A, 0484 Oslo

Foto Shutterstock

ISBN 978-82-327-0313-5
ISSN 1892-2597 (online)

www.nifu.no

Forord

Denne rapporten presenterer en studie av fremtidig tilbud på og etterspørsel etter IKT-sikkerhetskompetanse basert på framskrivningsmodeller utarbeidet av SSB. Oppdragsgiver har vært Justis- og beredskapsdepartementet, og oppdraget er et ledd i å opparbeide et solid kunnskapsgrunnlag for fremtidig tilbud av og etterspørsel etter IKT-sikkerhetskompetanse.

Prosjektet har vært gjennomført av forskerne Cathrine Tømte, Terje Næss, Trude Røsdal og Michael S. Mark (prosjektleder) med bidrag fra forskningsassistent Even Larsen, alle ved NIFU. I tillegg har Henrikke Flittig Aardalen, masterstudent fra studieretning Kommunikasjon, design og læring (KDL) ved Institutt for pedagogikk, Universitetet i Oslo, assistert under deler av datainnsamlingene.

Vi takker alle informanter som har bidratt i prosjektet. Konklusjoner og anbefalinger er forfatternes egne.

Oslo, desember 2017

Sveinung Skule
Direktør

Nicoline Frølich
Forskningsleder

Innhold

Sammendrag

IKT-sikkerhet er en sentral utfordring på alle samfunnsnivåer; for enkeltindivider, næringsliv, offentlig sektor, nasjonal infrastruktur og samfunnssikkerhet generelt. Mange peker på at utfordringer knyttet til IKT-sikkerhet øker; i dag er for eksempel IKT-kriminalitet den største økonomiske kriminalitetsformen i Storbritannia.

Formålet med denne studien har vært å frambringe oppdatert kunnskap om tilgangen på IKT-sikkerhetskompetanse, høyere utdanning/spesialistkompetanse på minimum bachelornivå[1], sett i forhold til arbeidslivets framtidige behov for slik kompetanse (både offentlig og privat sektor).

Rapporten omfatter to delstudier. Del 1 (kapittel 2 og 3) omfatter en framskrivning av behovet for IKT-sikkerhetskompetanse. Del 2 (kapittel 4 og 5) undersøker hva ulike samfunnsaktører legger i begrepet IKT-sikkerhet og ikke minst hvordan de vurderer fremtidig behov for slik kompetanse.

Basert på framskrivninger av tilbuds- og etterspørselssiden finner vi at det i år 2030 vil være en etterspørsel etter personer med IKT-sikkerhetskompetanse på vel 15 000. Tilgangen på IKT-sikkerhetskompetanse vil i samme år være på knapt 11 000. Dermed vil det i år 2030 være et gap på 4 100 personer med IKT-sikkerhetskompetanse. For å lukke dette gapet må tilbudssiden økes med vel en tredjedel, eller nærmere 37 prosent. Det er viktig å understreke at dette er framskrivninger og må tas med forbehold. Våre informanter peker likeledes på et behov for slik kompetanse her og nå samt i tiden som kommer. Det er derfor viktig å øke tilbudet av både grunnutdanning og etter- og videreutdanninger på fagfeltet og styrke kontakten mellom utdanningene, myndighetene og arbeidslivet.

Kort om studien

Denne studien presenterer den første konkrete framskrivningen av tilgang på og behov for IKT-sikkerhetskompetanse. Studien bygger på kjente framskrivningsmodeller for hele den norske arbeidsstyrken, modellen MODAG for etterspørselsframskrivningene og mikrosimuleringsmodellen MOSART for tilbudsframskrivningene. Opplysninger om opptak og gjennomføring er hentet fra NSDs Database for statistikk om høgre utdanning (DBH). I tillegg har vi gjennomført 18 intervjuer for å få utdypet funnene fra den kvantitative framskrivningen og adressere mulige innsatsområder for å dekke eventuelle gap.

MOSART og MODAG anses generelt som solide modeller for framskrivninger, men som alltid må framskrivninger anses som et estimat med en viss usikkerhet. I denne studien er fokus på IKT-sikkerhetskompetanse, som utgjør en relativt sett liten populasjon. En mindre populasjon er mer sensitiv overfor plutselige endringer. Det kan for eksempel forekomme endringer i antall studenter eller

[1] Fagskoler tilbyr også kurs i IKT-sikkerhet. Ifølge DBH var det i 2017 249 studenter på kurs som hadde IKT-sikkerhet i navnet.

markante endringer i etterspørselen som følge av et endret trusselbilde. En mindre populasjon vil altså ha økt usikkerhet ved framskrivninger.

Begrepet IKT-sikkerhet

Begrepet IKT-sikkerhet defineres vanligvis som evnen til å forebygge, oppdage og håndtere tre typer hendelser. UNINETT[2] definerer disse som:

- Brudd på konfidensialiteten, det vil si at uvedkommende får innsyn i beskyttelsesverdig informasjon.
- Brudd på integriteten, det vil si at informasjon og/eller systemer endres, skades eller slettes på uautoriserte eller utilsiktede måter.
- Brudd på tilgjengeligheten, det vil si at informasjon og/eller systemer går tapt eller er utilgjengelige når behovet er der.

IKT-sikkerhet omfatter slik flere nivåer; makronivå, som her kan forstås som samfunnet som helhet inklusiv myndighetene og myndighetsaktører, mesonivå, som kan forstås som organisasjoner, utdanningsinstitusjoner og arbeidsliv, og mikronivå som kan forstås som individnivå. Utfordringene er mange og komplekse, og situasjonen endrer seg i takt med at teknologien utvikles. Generelt tegnes dog et bilde med økende utfordringer.

IKT-sikkerhet høyt på agendaen

Det er derfor også igangsatt en rekke tiltak for å møte utfordringene knyttet til IKT-sikkerhet. I 2013 etablerte Difi et kompetansemiljø for informasjonssikkerhet. I 2014 nedsatte regjeringen et utvalg som skulle kartlegge samfunnets digitale sårbarhet. Utvalget skulle foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Lysne-utvalget leverte sin utredning høsten 2015; NOU 2015:13 Digital sårbarhet – sikkert samfunn. Utvalget pekte på en fremtidig mangel på arbeidskraft når det gjelder IKT-sikkerhet, og på den bakgrunn arbeides det nå med en IKT-sikkerhetskompetansestrategi for å styrke både utdanning og forskning på dette fagområdet.

Innenfor universitets- og høgskolesektoren har vi de siste årene sett en etablering av flere ekspertmiljø og/eller sentra med spesialisering innenfor ulike områder av det som omfatter IKT generelt og IKT-sikkerhet spesielt. Både ved NTNU, Universitetet i Bergen, Høgskolen i Oslo og Akershus og i et samarbeid mellom NTNU og Nord universitet er det særskilte satsinger for å styrke utdanning og forskning innen IKT-sikkerhet.

Antall studenter og uteksaminerte kandidater øker

I perioden fra 2012 til 2016 ser vi en betydelig økning i antall studenter og kandidater på studier der hovedfokus er IKT-sikkerhet og som utdanner såkalte IKT-sikkerhetsspesialister. Både antall studenter og kandidater dobles i perioden. I tillegg ser vi en tilsvarende økning i IKT-studier med kurs i IKT-sikkerhet der kandidatene kan kalles IKT-sikkerhetsgeneralister. Økningen er ikke så veldig markant, men ligger stadig på mer enn 40 prosent for antall studenter og mer enn 60 prosent for antall kandidater.

Andelen av både studenter og kandidater på studieprogram spesielt innrettet mot IKT-sikkerhet er imidlertid lav. Andelen IKT-sikkerhetsspesialister ligger på rundt 8–11 prosent av alle som tar utdanning som inneholder et minimum enkeltfag i IKT-sikkerhet. Hvorvidt det er en utfordring med hensyn til fremtidens etterspørsel, kan vi ikke svare på i denne studien. Men det er opplagt en potensiell utfordring.

I 2030 vil det være 4 100 ubesatte IKT-sikkerhetsstillinger

Til tross for den betydelige veksten i studenter og uteksaminerte kandidater er gapet mellom tilgang og behov økende. Våre framskrivninger peker på at det allerede per i dag er et gap mellom tilgang og behov, og dette gapet vil øke frem mot år 2030. Våre estimater peker på en underdekning på 4 100

[2] (UNINETT, s.7 (2017))

personer med IKT-sikkerhetskompetanse. Dette er et tall som selvsagt må tas med forbehold. Men tallet må samtidig tas på alvor. Vi har i våre framskrivninger forsøkt å innarbeide økningen i antall studenter og uteksaminerte kandidater, men allikevel ser vi et betydelig udekket behov.

Sammenlignbare land har også fokus på manglende IKT-sikkerhetskompetanse

Også i Danmark, Sverige og Nederland har man gjort analyser av behovet for økt IKT-sikkerhetskompetanse. I Danmark og Sverige pekes det på akutte behov, mens behovet tilbake i år 2014 i Nederland ble vurdert av nederlandske forskere til å være noe mindre akutt. Dette kan ha endret seg siden da. De tre landene har nasjonale strategier for å håndtere utfordringer knyttet til IKT-sikkerhet, herunder IKT-sikkerhetskompetanse. Strategiene varierer i konkretiseringsgrad og ambisjonsnivå. Den mest ambisiøse og konkrete strategien har Storbritannia, hvor det avsettes 16 000 mill. NOK frem til 2021 for å håndtere IKT-sikkerhetsutfordringene.

Akutt behov og løsninger på kort og lang sikt

Gjennom våre intervjuer med 18 norske aktører pekes det på et akutt behov; lønningene skyter i været, og mange kandidater har jobb 12–18 måneder før avsluttet mastergrad. Det er tegn på en betydelig ulikevekt mellom tilbud og etterspørsel. Flere studieplasser er en viktig del av løsningen. Samtidig synes etter- og videreutdanningstilbudet å være begrenset. Dette tilbudet bør økes, og det bør undersøkes nærmere om de rette insentivene for å tilby og etterspørre etter- og videreutdanning innen IKT-sikkerhet er på plass.

IKT-sikkerhet er et område som må bygge på et sterkt teoretisk fundament. Men samtidig er den praksisnære og anvendelsesorienterte undervisningen og forskningen viktig. IKT-sikkerhet er et felt som er komplekst, tverrfaglig og som utvikler seg hurtig. Derfor må en økt forskningsinnsats ikke alene bygge på tidligere meritter i form av publisering og sitering, men i høy grad bygge på samspill mellom myndigheter, næringsliv og akademia. For å styrke den praksisnære undervisningen bør det utredes hvordan eksterne undervisere kan bidra til å øke kvaliteten og omfanget på undervisningen.

Etterskrift

Parallelt med ferdigstillingen av rapporten har den offentlige oppmerksomheten om temaet IKT-sikkerhet økt, ikke minst har det vært bred oppmerksomhet om behovet for kryptologer. Temaet er diskutert i Stortinget, og i forbindelse med budsjettforliket for 2018. I den forbindelse har konkrete innsatser knyttet til IKT-sikkerhet blitt lagt fram. Det dreier seg om tiltak som kan motvirke manglende overganger fra master- til doktorgrad og videre karriereløp innen IKT-sikkerhet. Blant tiltakene er forskerlinje innen informatikk og en økning på 50 rekrutteringsstillinger. I budsjettforliket ble det enighet om 500 studieplasser innen IKT-utdanning i 2018, og Kunnskapsdepartementet vil be om at IKT-sikkerhet blir prioritert.

Det er slik satt fokus på å øke antallet personer med IKT-sikkerhetskompetanse. Flere av de tiltaksområdene vi peker på i foreliggende rapport for å øke tilgangen på både IKT-sikkerhets-generalister og -spesialister, er adressert i det som er lagt fram. Dette reiser også spørsmål rundt hvordan man skal klare å rekruttere til de 50 rekrutteringsstillingene, når det allerede i dag er meget vanskelig å rekruttere norske eller nordiske kandidater til slike stillinger. En annen problemstilling er hvorvidt det er tilstrekkelig med undervisningskompetanse til å følge opp økningen av IKT-studieplasser. Ifølge regjeringen økes det samlede tallet på IKT-studieplasser med 1 250 i 2017 og 2018 til sammen. Avslutningsvis vil vi peke på at disse satsingene neppe løser dagens eller morgendagens utfordringer. De som påbegynner IKT-studiet i 2018, er ferdige kandidater tidligst i år 2022. De som påbegynner ph.d.-studiet i 2018, er ferdige doktorander tidligst i år 2021. Det er positivt at de langsiktige utfordringene rundt mangelen på IKT-sikkerhetskompetanse imøtegås, men det er fortsatt et spørsmål hva som kan gjøres på kort sikt for å møte den nåværende ubalansen mellom tilbud og etterspørsel.

1 IKT-sikkerhet høyt på agendaen

Målet med foreliggende studie er å gi en oversikt over tilgang på adekvat IKT-sikkerhetskompetanse og dernest vurdere denne tilgangen i lys av (samfunnets) arbeidslivets behov for slik kompetanse.

IKT-sikkerhet er et viktig satsingsområde for regjeringen som omfatter individ-, organisasjons- og samfunnsnivå i alle sektorer. I tillegg må IKT-sikkerhet ses i sammenheng med regjeringens øvrige arbeid med samfunnssikkerhet. Slik vil foreliggende studie, som ser på tilbudet av og etterspørselen etter IKT-sikkerhetskompetanse, inngå som en del av regjeringens omfattende arbeid knyttet til IKT-sikkerhet og samfunnssikkerhet som sådan. I tillegg er foreliggende studie en del av arbeidet med en nasjonal kompetansestrategi for IKT-sikkerhet. Dette arbeidet ble besluttet iverksatt i forbindelse med Samfunnssikkerhetsmeldingen Meld. St. 10 (Justis- og beredskapsdepartementet, Regjeringen Solberg, 2016).

Rapporten omfatter to delstudier. De to delstudiene sammenfattes i kapittel 2, men del 1 (kapittel 3 og 4) omfatter en framskrivning av behovet for IKT-sikkerhetskompetanse. Del 2 (kapittel 4 og 5) undersøker hva ulike samfunnsaktører legger i begrepet IKT-sikkerhet, og ikke minst hvordan de vurderer fremtidig behov for slik kompetanse. En nærmere beskrivelse av studiens design, metodiske tilnærminger og datagrunnlag finnes som vedlegg.

1.1 Begrepet IKT-sikkerhet

Før vi beskriver vårt arbeid mer i detalj, vil vi reflektere over hva vi helt konkret legger i begrepet IKT-sikkerhet, og hva IKT-sikkerhet betyr avhengig av i hvilke deler av, og på hvilke nivåer i samfunnet vi beveger oss. Et neste steg er å se på hvordan universitets- og høgskolesektoren definerer IKT-sikkerhetskompetanse i sine utdanningstilbud i lys av hvordan vi så langt har definert og organisert etterspørselssidens forståelse av IKT-sikkerhet.

IKT-sikkerhet defineres vanligvis som evnen til å forebygge, oppdage og håndtere tre typer hendelser. UNINETT definerer disse som

- Brudd på konfidensialiteten, det vil si at uvedkommende får innsyn i beskyttelsesverdig informasjon.
- Brudd på integriteten, det vil si at informasjon og/eller systemer endres, skades eller slettes på uautoriserte eller utilsiktede måter.
- Brudd på tilgjengeligheten, det vil si at informasjon og/eller systemer går tapt eller er utilgjengelige når behovet er der.

(UNINETT, s 7 (2017))

Selv om UNINETT har ansvaret for teknologisk infrastruktur til universitets- og høgskolesektoren, synes ovennevnte inndeling av typer hendelser å være såpass brede at de også kan omfatte IKT-sikkerhet for samfunnet generelt.

IKT har skapt store endringer de siste tiårene, og samfunnet, næringslivet og privatsfæren er i økende grad avhengig av IKT. På mange måter utgjør IKT nå grunnmuren for all samhandling på tvers av sektorer. I NOU 2015: 13, *Digital sårbarhet – sikkert samfunn* påpekes det at denne utviklingen har gjort IKT til en strategisk sikkerhetsutfordring:

> *Infrastrukturen som ligger til grunn for at tjenestene fungerer, har blitt kritisk for at samfunnet skal fungere normalt. Den raske utviklingen av IKT-teknologi fører til rask endring og fornyelse av eksisterende digitale løsninger. Ved både tilsiktede (kriminalitet, terror, spionasje) og ikke-tilsiktede hendelser (ulykker, naturhendelser) er det behov for å beskytte informasjonen og sørge for at våre nettverk og systemer er sikre og stabile til enhver tid.*
>
> NOU 2015: 13 Digital sårbarhet – sikkert samfunn

IKT-sikkerhet omfatter slik flere nivåer; makronivå, som her kan forstås som samfunnet som helhet inklusiv myndighetene og myndighetsaktører, mesonivå, som kan forstås som organisasjoner, utdanningsinstitusjoner og arbeidsliv, og mikronivå, som her kan forstås som individnivå. IKT-sikkerhet innebærer med andre ord at ulike utfordringer må håndteres på ulike måter av ulike aktører.

1.2 IKT-sikkerhet en utfordring på mange nivåer

Utfordringene er mange og komplekse, og situasjonen endrer seg i takt med at teknologien utvikles. Trusselbildet omfatter alle nivåer, fra samfunnsnivå til enkelt individ og har ulik betydning på de ulike nivåene. Formålet med dette avsnittet er ikke å foreta en litteraturgjennomgang av akademisk forskning, men i stedet å presentere nyere eksempler på IKT-sikkerhetsutfordringer slik de er kommet frem i rapporter og fremhevet gjennom media.

Landets e-tjeneste presenterte tidligere i vinter sin årlige trusselvurdering. Av den fremgikk det at teknologisk avansert militær aktivitet utgjør en sentral trussel for landet. Rapporten ble publisert kun få dager etter at det var blitt kjent at PST, Forsvarsdepartementet og Arbeiderpartiet hadde vært utsatt for et forsøk på hacking, fra en hackergruppe som skal være tilknyttet russiske myndigheter (www.nrk.no, 03.02.2017).

I 2015 påpekte Riksrevisjonen alvorlige svakheter ved sikkerheten i informasjonssystemene i flere etater, deriblant Politi- og lensmannsetaten, Arbeids- og velferdsetaten og Brønnøysundregistrene. Riksrevisjonen fremhevet den gang at større forbedringer forutsetter kompetanse og systematisk arbeid (www.digi.no,21.10.2015).

Også nasjonale infrastrukturer er tematisert når det er tale om IKT-sikkerhet. For å beskytte seg mot hackerangrep foretok man i 2013 blant annet en analyse av norske kraftselskap og deres håndtering av IKT-sikkerhet og fant flere svakheter knyttet til rutiner og systemer (www.tu.no, 18.01.2013).

Tidligere i år kritiserte media myndighetenes håndtering av sensitive data, da det ble kjent at landets nødnett driftes av et selskap plassert i India (www.nrk.no, 07.02.2017). I fjor problematiserte NITOs president, Trond Markussen, at Helse Sør-Øst har satt ut sin IKT-drift til et privat selskap plassert i Bulgaria, noe som innebærer at sensitive data, som helsedata, kan befinne seg utenfor landets grenser (www.nito.no, 14.11.2016). Markussens bekymringer var ingen dyster fantasi. Denne våren avdekket NRK at IT-arbeidere fra både Øst-Europa og Asia har hatt tilgang til sensitiv pasientinformasjon i Helse Sør-Øst, og i praksis har disse hatt mulighet til å hente ut pasientdata til 2,8 millioner nordmenn; «NRKs kilder forteller at flere titalls utenlandske IT-arbeidere har hatt slik tilgang og at mange har hatt utvidede rettigheter, større enn mange av de norske IT-teknikerne» (www.nrk.no, 8.5.2017). Konsekvensene er omfattende, og mens helsepersonale frykter at pasienter vil holde

tilbake personlig informasjon under kommende konsultasjoner, har pasientombudet bedt om full innsikt i hva som har skjedd. Teknologidirektør har dessuten trukket seg fra jobben, og et revisorfirma skal granske hva som egentlig har skjedd (ibid).

Petroleumsbransjen har også blitt kritisert for manglende bevissthet og rutiner for IKT-sikkerhet. Senest i desember 2016 var Statoil i media fordi det ble avdekket at opptil 100 IT-arbeidere i India hadde full tilgang til brannmurene på Statoils anlegg. En mulig konsekvens kunne i verste fall innebære at man fra India iverksatte stans eller sabotasje av produksjon (www.nrk.no, 21.12.2016).

Innenfor universitets- og høgskolesektoren har UNINETT nylig publisert en IKT-strategi for norsk UH-sektor, der man presenterer ulike tiltak som skal ivareta sektorens sammensatte utfordringer knyttet til drift og forvaltning av ulike systemer og tjenester, og perspektiver på hvordan trusselbildet kan se ut nå og i fremtiden.

Politidirektoratet har siden 2015 utarbeidet en særskilt trusselvurdering for IKT-kriminalitet. Seneste rapport (Politidirektoratet, 2017) peker på at trusselen fra IKT-kriminalitet stiger i takt med økt digitalisering i samfunnet og den generelle teknologiutviklingen. Rapporten peker dessuten på at den økte trusselen og utviklingen innen IKT-kriminalitet kommer til å påvirke Norge og nordmenn.

Også på individnivå er IKT-sikkerhet vektlagt. Mye arbeid legges ned i å sikre et godt personvern og sensitive opplysninger, blant annet knyttet til utdanning, arbeidsliv og helse. Men også her finnes utfordringer, slik eksemplet ovenfor fra Helse Sør-Øst viste.

Eller som når vi gjennom media har vært vitne til at DNBs nettbank har vært nede denne vinteren. Som en sentral aktør innen bank og finans er det flere som kritiserer banken for ikke å ha bedre sikkerhetsløsninger for sine brukere. Interesseorganisasjonen IKT-Norge mener nettbanker må anses som infrastruktur som er kritisk for samfunnet, og at det derfor må stilles strenge krav til oppetid og stabilitet (www.nrk.no, 16.03.2017).

Selv om utfordringene er mange og trusselbildet endrer seg i takt med teknologiutviklingen, er det iverksatt mange tiltak og grep fra myndighetenes side for å holde oppmerksomheten oppe rundt IKT-sikkerhet. Flere NOU-er, stortingsmeldinger og utvalg har arbeidet med ulike sider knyttet til IKT-sikkerhet for samfunn, arbeidsliv og for den enkelte. Siden 2004 har Direktorat for samfunn og forvaltning, Difi, årlig kartlagt IKT-sikkerheten i staten, og et hovedfunn i 2014 var at beredskapen er svak og at mye av forklaringen ligger hos ledelsen som engasjerer seg lite i IKT-sikkerhet (www.tu.no, 07.04.2014).

Også internasjonalt er det betydelig fokus på utfordringer rundt IKT-sikkerhet. Teknologisk Institut i Danmark peker i samarbeid med Fraunhofer (2012) på:

> *«By far, security is predicted to become one of the key skills due to increase in the amount of data and the critical character of data stored in the cloud»*

I Storbritannia økte andelen av bedrifter som ble utsatt for IKT-kriminalitet fra 35 prosent i perioden 2012–2013 til 55 prosent i perioden 2014–2015. Den kraftige økningen i kriminalitet står i kontrast til at andre kriminalitetsformer stuper. Som det fremkommer av PriceWaterhouseCoopers (PwC) undersøkelse «Global Economic Crime Survey (2016)», er IKT-kriminalitet nå den største økonomiske kriminalitetsformen i Storbritannia.

Basert på samme PwC-undersøkelse peker danske virksomhetsledere også på massive IKT-kriminalitetsutfordringer. I undersøkelsen basert på 300 respondenter svarer:

- 69 prosent at de har vært utsatt for cyberangrep de siste 12 månedene
- 67 prosent at de har vært utsatt for utpressing som eksempelvis ransomware de siste 12 månedene
- 65 prosent at de er mer bekymret for cybertrusselen nå enn for 12 måneder siden.

I rapporten «Cloud Security» (Information Security Community on Linkedin, 2016) pekes det på at sikkerhet er nøkkelfaktoren for å utnytte sky-baserte løsninger. Basert på svar fra 2.200 respondenter svarer 91 prosent (rundt 2.000 respondenter) at de er bekymret når det gjelder å anvende sky-baserte løsninger på grunn av utfordringer med IKT-sikkerheten.

Videre pekes det på store utfordringer med å få tak i nok personell med kompetanse til å møte økningen i IKT-kriminalitet. Global Information Security Workforce Study (2017) har gjennomført en omfattende global survey og fått svar fra 19.641 respondenter. Her pekes det på at det allerede i år 2022 vil mangle 1.800.000 IKT-sikkerhetsmedarbeidere. Dette er selvsagt et tall som må tas med et forbehold. Det baserer seg på synsing blant respondentene, og det er en risiko for at de overvurderer fremtidige behov. Omvendt peker undersøkelser fra Norge på at det generelt er en betydelig mangel på IKT-medarbeidere. En stor del av disse vil trolig være innen IKT-sikkerhet, og det er forventet at dette tallet vil øke.

Den nasjonale cyber-sikkerhetsstrategien i Storbritannia peker på utfordringer med IKT-sikkerhetskompetanse. Her fremheves det at … «*Recruitment of individuals with technical cyber security skills was considered difficult by the majority of participants. »*, Department for Business Innovation and Skills (2014)

Et INTERREG-prosjekt skal fra 2015 til 2019 undersøke mulighetene for etter- og videreutdanning innen IKT-sikkerhet. Prosjektets utgangspunkt er at etterspørselen etter personell med IKT-sikkerhetskompetanse vokser med 3,5 ganger den generelle etterspørselen etter personell med IKT-kompetanse og med 12 ganger den generelle etterspørselen etter arbeidskraft, se http://database.centralbaltic.eu/project/5 for mer informasjon.

Lysne-utvalget (2015) peker på at … «*IKT-sikkerhet er et av områdene der det forventes et særlig behov for kompetanse*.» Og videre heter det: «*Det er bred enighet blant infrastruktureiere og bransjeorganisasjoner om at det er en generell mangel på personer med IKT-sikkerhetskompetanse i samfunnet, og at det er utfordrende å rekruttere til denne typen stillinger.*» Til slutt konstateres det at det er bred enighet om at det er et gap mellom tilbud og etterspørsel etter IKT-sikkerhetskompetanse og at det er en økende etterspørsel.

I en undersøkelse fra 2017 peker PwC på at ledelsen i stadig større grad involveres i spørsmål om cybersikkerhet, (PriceWaterhouseCoopers, 2017)). Dette sammenfaller formentlig med at cyberkriminalitet blir sett på som en økende utfordring. I tillegg viser Cyber Crime Survey (PriceWaterhouseCoopers, 2017) at norske bedrifter i løpet av de kommende 18 måneder forventer å øke sine budsjetter for kontroll og forebygging av cyberkriminalitet med 26 prosent. Dette vil sette ytterligere press på etterspørsel etter personer med IKT-sikkerhetskompetanse.

1.3 Norske tiltak for å møte utfordringer knyttet til IKT-sikkerhet

Myndighetene har som nevnt hatt IKT-sikkerhet på agendaen i flere år. Som et tiltak i realiseringen av Nasjonal strategi for informasjonssikkerhet, skal for eksempel Difi arbeide for en styrket og mer helhetlig tilnærming til informasjonssikkerhet i statsforvaltningen. I 2013 etablerte Difi et kompetansemiljø for informasjonssikkerhet. Et av fokusområdene er å styrke informasjonssikkerheten gjennom økt bruk av styringssystemer for informasjonssikkerhet. I rapport 2012:15 (2012) har Difi sett på erfaringer med innføring av slike systemer, og gir råd om innføringen (www.difi.no, 9.5.2017).

I tillegg til at man har økt oppmerksomhet knyttet til IKT-sikkerhet innenfor statsforvaltningen, har myndighetene også initiert flere utredninger om hvordan samfunnet best kan forberede seg på utfordringer knyttet til IKT-sikkerhet.

I 2014 nedsatte regjeringen et utvalg som skulle kartlegge samfunnets digitale sårbarhet. Utvalget skulle foreslå konkrete tiltak for å styrke beredskapen og redusere den digitale sårbarheten i samfunnet. Lysne-utvalget leverte sin utredning høsten 2015; NOU 2015:13 *Digital sårbarhet – sikkert*

samfunn. Utvalget pekte på fremtidig mangel på arbeidskraft når det gjelder IKT-sikkerhet og foreslo en kompetansestrategi for både å styrke utdanning og forskning på dette fagområdet. I februar 2016 nedsatte Forsvarsdepartementet et utvalg (Lysne II) for å utrede sentrale problemstillinger knyttet til en etablering av digitalt grenseforsvar. Dette spesifikke temaet har tidligere vært berørt av en annen ekspertgruppe, ledet av Professor Rolf Tamnes, som leverte rapporten "Et felles løft" (2015). Lysne II-utvalgets anbefalinger ble sendt på høring og møtte til dels kritikk, spesielt med tanke på forslaget om å etablere et digitalt grenseforsvar, fordi en slik innretning kan komme i konflikt med personvernlovgivningen.

Høsten 2016 bevilget Stortinget penger til 500 nye IT-studieplasser. Av disse kan vi anta at en del omfatter IKT-sikkerhet. I tillegg ble 65 studieplasser øremerket til IKT-sikkerhet i 2016 (Revidert nasjonalbudsjett). Direktør for IKT-Norge, Heidi Austlid, påpeker at de digitale næringene er underbemannet, og at behovet for IT-folk bare vil øke i årene som kommer. De trengs både i næringslivet og offentlig sektor. Dessuten avdekket en måling IKT-Norge gjorde for to år siden 6.000 ubesatte stillinger i bransjen (DN 28.4.2017). Den IT-kompetansen som her etterlyses, er generell, men vi kan likevel anta at behovet for IKT-sikkerhetskompetanse inngår i denne generelle tilnærmingen, uten at omfanget av en slik spesialkompetanse er konkretisert spesielt.

Innenfor UH-sektoren har vi de siste årene sett etablering av flere ekspertmiljø og eller sentra med spesialisering innenfor ulike områder av det som omfatter IKT generelt og IKT-sikkerhet spesielt. Noen av disse er:

Forskningssenteret for informasjons- og kommunikasjonssikkerhet; Simula@UiB

- Etablert 2016
- Samarbeid mellom forskningsgruppen ved Selmersenteret ved UiB og forskere ved Simula.
- Mål: øke sikkerhetsekspertisen i Norge gjennom forskning og utdanning. Spesialiserer seg på kryptologi og informasjonsteori.
- Aksjeselskap eid av Universitetet i Bergen (UiB) og Simula Research Laboratory.
  Støtte fra Samferdselsdepartementet og eierne. Senteret skal i tillegg hente inn midler fra Norges forskningsråd, EU og andre kilder.
  Nettsted: www.simula-uib.com

Center for Cyber and Information Security

- Etablert 2014
- Forskningssenter for cyber- og informasjonssikkerhet, Gjøvik, NTNU.
- Bredt samarbeid mellom en rekke aktører innenfor akademia, næringsliv og offentlig forvaltning.
- Initiativtakerne inkluderer Nasjonal sikkerhetsmyndighet (NSM), Politidirektoratet, Politiets sikkerhetstjeneste (PST), Cyberforsvaret, Forsvarets Forskningsinstitutt (FFI), Telenor, Statkraft, Statnett og Eidsiva, Økokrim, Kripos, Nasjonalt ID-senter, PwC og Oppland fylkeskommune.
- Mål: møte langsiktige digitale utfordringer. Bidra til å utvikle ny kompetanse på et område som har blitt kritisk for alle samfunnsaktører, og legge til rette for kunnskapsutveksling mellom forskningsmiljøer og anvendelsesmiljøer. Gjennom samarbeidet i CCSI skal politiet bli bedre i stand til å forebygge og bekjempe datakriminalitet, mens studentene skal tilbys mer relevant undervisning ved å få større inngrep med praktiske problemstillinger.
- Politiet har finansiert tre av senterets professorater.
- JD og SHD gir en årlig basisfinansiering. Stortinget ga en føring om personvern.

Nytt utdannings- og forskningssenter for digitalisering - HiOA

- Etablert 2016
- Høgskolen i Oslo og Akershus (HiOA) og Simula Research Laboratory.
- Mål: å levere flere høyt kvalifiserte kandidater på bachelor-, master- og doktorgradsnivå innenfor blant annet kunstig intelligens, cybersikkerhet og stordata.

EXcITEd – Excellent IT Education

- Etablert 2016
- SFU, et samarbeid mellom NTNU (Trondheim og Gjøvik) og Nord universitet.
- Mål: å bringe norsk høyere utdanning innenfor informasjonsteknologi til verdenstoppen.
- Senteret skal jobbe for at flere studenter velger informasjonsteknologi som utdanningsvei og vil også utvikle nye informasjonsteknologiske verktøy til bruk i læring på tvers av fagfelt.
- Gjøre en forskjell når det gjelder å rekruttere studenter, særlig jenter, til data- og IT-studier.

Det settes altså i verk tiltak for å styrke kompetanse- og kunnskapsnivået innen IKT-sikkerhet i Norge. Et relevant spørsmål her blir da om det gjøres nok; om innsatsen er ambisiøs nok og om mengden ressurser som allokeres til å styrke kompetanse- og kunnskapsnivået, er tilstrekkelig. Det er videre et spørsmål om kandidatene oppnår den kompetansen som etterspørres.

Dette er spørsmål vi drøfter i den resterende delen av rapporten

Rapporten er bygget opp på følgende måte: I kapittel 2 presenteres sentrale funn og anbefalinger for å dekke et fremtidig gap mellom tilbud og etterspørsel innen IKT-sikkerhetskompetanse. Kapittel 3 gir en oversikt over norske utdanninger som i større eller mindre grad tilbyr kurs i IKT-sikkerhet på minimum bachelornivå, og kapittel 4 presenterer en kvantitativ framskrivning av tilbud på og etterspørsel etter personer med IKT-sikkerhetskompetanse på minimum bachelornivå. Kapittel 5 presenterer perspektiver fra norske aktører innen IKT-sikkerhet, mens kapittel 6 har fokus på status for IKT-sikkerhetskompetanse i Danmark, Sverige, Nederland og Storbritannia.

2 Sentrale funn og anbefalinger

Hovedformålet med prosjektet har vært å bidra til et datagrunnlag for og oppdatert kunnskap om tilgangen på IKT-sikkerhetskompetanse på høyere utdanningsnivå, sett i forhold til arbeidslivets framtidige behov (både offentlig og privat sektor) for slik kompetanse. Rapporten drøfter både generalist- og spesialkompetanse. Vår studie har tatt utgangspunkt i en kvantitativ framskrivning basert på ulike datakilder; MOSART, MODAG, registerdata og opplysninger om opptak og gjennomføring fra NSDs Database for statistikk om høgre utdanning (DBH). I tillegg har vi gjennomført 18 intervjuer for å utdype funnene fra den kvantitative framskrivningen og for å adressere mulige innsatsområder for å dekke eventuelle gap.

Studiens første del presenterte tall og framskrivninger som viser at det i år 2030 er et gap på 4 100 personer med den aktuelle kompetansen. Dette tallet er det selvfølgelig knyttet en del usikkerhet til, men vi kan dog slå fast at det ifølge modellene er et stort gap mellom tilbud på og etterspørsel etter slik kompetanse. Samtidig viste tallene at rundt 8 000 personer i år 2016 hadde adekvat utdanning, mens etterspørselen i modellene lå på rundt 10 000 personer. Vi har altså et underskudd på om lag 2 000 personer allerede i dag.

Vi gjorde ingen distinksjoner mellom forskjellige typer IKT-sikkerhetskompetanse. I stedet bygger modellene på de personene som har tatt utdanning på høyere nivå, der IKT-sikkerhet er en større eller mindre del av utdanningen.

På globalt nivå er det estimert at det i år 2022 vil være et underskudd på 1 800 000 personer med IKT-sikkerhetskompetanse på verdensbasis (Frost & Sullivan, 2017). Hvorvidt dette tallet er i overensstemmelse med de estimater vi gjør, er vanskelig å vurdere. Ser vi på naturlig sammenlignbare land, finner vi at i hvert fall det omtrentlige antallet personer med IKT-sikkerhetskompetanse stemmer noenlunde med vår studie:

- I Danmark estimerer vi at antallet personer med IKT-sikkerhetskompetanse ligger på 8–9 000 personer. Dette er basert på en analyse av stillingsannonser innen IKT-sikkerhet gjennomført av Højbjerre Brauer Shultz. Ved å kartlegge antallet stillingsannonser rettet mot IKT-sikkerhetskompetanse kan vi identifisere mangelen på personer med IKT-sikkerhetskompetanse (Højbjerre Brauer Schultz, 2017).

- I Sverige peker en nylig offentliggjort survey på at det finnes minimum 5 000 personer med IKT-sikkerhetskompetanse. Det bygger på svar fra 202 bedrifter. Totaltallet er trolig mye høyere, men hvor høyt er vanskelig å si.

- I Nederland estimerer vi antallet personer med IKT-sikkerhetskompetanse til å være 12–14 000 i år 2014. Det høye tallet avspeiler i noen grad at Nederlands befolkning er større enn

Norges og at Nederland har et større arbeidsmarked. Dog kunne man ha forventet at tallet var enda høyere. Estimeringen er gjennomført på bakgrunn av en forskningsrapport om behovet for IKT-sikkerhetskompetanse i Nederland (van Lakerveld, et al., 2014), som anvender samme metode som i den danske studien, nemlig opptelling av stillingsannonser rettet mot IKT-sikkerhetskompetanse.

Sverige har som det eneste av de ovennevnte land gjort vurderinger av fremtidig behov for personer med IKT-sikkerhetskompetanse. Her estimerer vi, på bakgrunn av tall fra analysen, at Sverige i år 2022 vil ha et underskudd på minst 1 785 personer med IKT-sikkerhetskompetanse, da tilbudssiden må økes med 35,7 prosent i år 2022 for å dekke behovet. De 1 785 bygger på at det per i dag finnes 5 000 personer med IKT-sikkerhetskompetanse, et tall som trolig er underestimert, og man antar derfor at gapet mellom tilbud og etterspørsel er enda større.

Den store etterspørselen etter og mangelen på IKT-sikkerhetskompetanse bekreftes av våre informanter. Gjennom intervjuer har vi bedt dem vurdere dagens og fremtidens behov for IKT-sikkerhetskompetanse. Samlet peker informantene på at det er et betydelig underdekket behov per i dag. Og utviklingen i både teknologi, antall enheter som er på nett, og økt organisering og profesjonalisering blant IKT-kriminelle gjør at behovet øker.

Det relevante spørsmål er da, hvordan fylle kompetansegapet? Basert på våre intervjuer og hva våre informanter har pekt på, har vi her forsøkt å sammenfatte hva som kanskje kan være noen mulige løsninger på utfordringene vi står overfor. Hvert av løsningsforslagene er på overordnet nivå, og det vil kreve en dedikert innsats blant relevante/aktuelle aktører for å implementere disse forslagene. De mulige løsningene er:

1. Vi trenger flere personer med IKT-sikkerhetsutdanning. Vi trenger flere generalister som tar fag innen IKT-sikkerhet som en del av en bredere IKT-utdanning. Disse vil kunne bidra til å fylle kompetansegapet bredt i både offentlig og privat sektor. Men vi trenger også flere spesialister, der IKT-sikkerhet er selve kjernen i utdanningen. Disse vil også kunne bidra til å fylle kompetansegapet, men like viktig vil det være at disse kandidatene tar forskerutdanning og senere blir fremtidens forskere og undervisere på feltet. Generalistene vil selvsagt også kunne gå forskerveien, men det vil antakelig være en mindre andel av disse som vil ta ytterligere spesialisering innen IKT-sikkerhet.

   Dersom flere skal ta IKT-utdanning, må det allokeres flere ressurser til utdanninger innen IKT og IKT-sikkerhet. Og det må stilles krav til utdanningsinstitusjonene om at tildelte ressurser faktisk går til å øke utdanningskapasiteten innen IKT-sikkerhet. Dette kan i noen grad innskrenke UoH-sektorens autonomi, men når det er snakk om en samfunnskritisk utfordring, må kanskje Kunnskapsdepartementet i større grad komme på banen med tydelige føringer på hva ekstra ressurser skal anvendes til.

2. Fortsette arbeidet med å utjevne kjønnsforskjeller. Vi ser at selv om det er en utbredt oppfatning at det jobbes intensivt med å utjevne kjønnsforskjeller innenfor dette feltet, så viser blant annet studenttallene at skjevfordelingen er like stor (og faktisk noe økende) som den var for 10–20 år siden. Når vi samtidig hører fra utdanningsinstitusjonene at de ønsker bedre kvalitet på søkerne, er det opplagt at det må satses på å få flere personer til å søke mot utdanninger innen IKT-sikkerhet, noe som innebærer at også flere kvinner må søke seg til disse fagområdene.

   I tråd med hva flere av våre informanter fremhever som spesielt viktig for å øke tilgangen til IKT-sikkerhetskompetanse, vil vi også understreke betydningen av å innføre IKT-sikkerhet og IKT tidligere i utdanningsløpet. Det vil si at allerede på videregående skole bør man tilby fag med IKT-sikkerhet, liksom det påpekes at programmering bør inngå i ungdomsskolen og til og med helt fra barnehagen.

3. Fortsette å styrke forskningsmiljøene og på lang sikt bygge nye. Det er utfordrende å trekke unge dyktige studenter til en forskerutdanning. Det er hard konkurranse med både offentlig sektor og næringsliv, som hver tilbyr høye lønninger og interessante fagmiljøer. Med utgangspunkt i tilbakemeldingene fra våre informanter vil vi peke på betydningen av å styrke eksisterende fagmiljøer og muligens etablere nye. En slik styrking av eksisterende fagmiljøer innenfor høyere utdanning i Norge vil være avgjørende for å klare å rekruttere både forskertalenter og allerede etablerte fagpersoner og forskere. I konkurranse med høye lønninger utenfor UH-sektoren mener våre informanter at et sterkt fagmiljø er UH-sektorens viktigste konkurransefortrinn.

   Forskning på IKT-sikkerhet bygger på et sterkt teoretisk fundament. Men det er også viktig å få med den anvendelsesorienterte og praksisnære delen av forskningen. Mangelfull forståelse av det komplekse teknologiske samspillet mellom sosiale og organisatoriske dimensjoner danner grunnlaget for IKT-kriminaliteten. De kriminelle går etter det svakeste leddet, og det er oftere menneskelige feil enn teknologiske som er avgjørende. Basert på tilbakemeldingene fra våre informanter anbefaler vi at styrking av forskningen og oppbygging av forskningsmiljøer ikke kun skjer ut fra tradisjonelle tellekanter, men også i samspill mellom kjerneaktører innen praksisfeltet.

4. Det kan overveies å bruke eksterne undervisere i høyere utdanning i større grad enn det som gjøres i dag. Eksterne undervisere kan eksempelvis hentes inn fra næringslivet eller offentlige myndigheter. I den grad det er mulig å rekruttere eksterne undervisere, vil det være med på å dekke behovet for å undervise som naturlig vil komme som følge av vårt forslag under punkt 1. Videre vil et slikt grep styrke den anvendelsesorienterte delen av den forskningsbaserte undervisningen. Det vil også kunne styrke nettverk og samarbeid mellom utdanningsinstitusjoner, næringsliv og myndigheter, noe som igjen vil kunne styrke den praksisnære forskningen (jf. også våre anbefalinger i punkt 3).

   Dersom man stiller krav til at eksterne undervisere skal ha utdanning på doktorgradsnivå, vil dette sannsynligvis innebære en utfordring, da tilgangen på personer med denne kompetansen på dette nivået er meget begrenset både innenfor og utenfor UH-sektoren.

5. En annen viktig tilnærming for å minske kompetansegapet er etter- og videreutdanning (EVU). Vi opplever det som påfallende at det er så få etter- og videreutdanningstilbud på IKT-området. Vi registrerer at det er enda færre EVU-tilbud innen IKT-sikkerhet. Det har ikke vært mulig for oss i dette prosjektet å gå nærmere inn på hvorfor det er så få tilbud, men dette bør selvfølgelig undersøkes nærmere

   Det bør legges bedre til rette for utvikling av et bredere EVU-tilbud innen IKT-sikkerhet, og eventuelle utfordringer når det gjelder rekruttering av forelesere, og også finansiering, må adresseres.

   Den teknologiske utviklingen innen IKT-kriminalitet skjer så fort at det vil være behov for å kunne oppgradere eksisterende kompetanse på en kontinuerlig måte. EVU innen IKT-sikkerhet vil trolig måtte spille en sentral rolle i å dekke kompetanseetterspørselen.

6. IKT-sikkerhet rommer også et betydelig næringspotensial, altså et område der det skapes arbeidsplasser i privat sektor. Det har ikke vært en del av temaet for vår studie, men når vi allikevel trekker det frem, skyldes det både våre informanter og særlig Storbritannias IKT-sikkerhetsstrategi. I den fremgår næringspotensialet til IKT-sikkerhet eksplisitt. Her har man også etablert et særskilt innovasjonsfond, som skal understøtte innovasjon innen IKT-sikkerhet.

   IKT-sikkerhet har ikke samme globale markedsstørrelse som helse eller energi. Men allerede nå øker det globale markedet for IKT-sikkerhetsløsninger og -tjenester kraftig, og det

forventes at markedet øker gjennomsnittlig 11 prosent i året frem til år 2022[3]. Man forventer altså at det globale markedet vokser fra rundt $120 000 millioner i 2017 til $232 000 millioner i år 2022. Norge vil med sin stabile politiske situasjon, sin troverdighet og tilnærmelsesvis nøytralitet i verdenspolitikken kunne stå som en sterk global tilbyder av IKT-sikkerhetsløsninger.

[3] Se: “Global Cyber Security Market, 2015–2021: By Solutions, Verticals, Network Security, Cloud Security, Wireless Security and Others” eller “Cybersecurity Market by Solution".

3 Norske utdanninger med fokus på IKT-sikkerhet

I dette kapitlet ser vi nærmere på antallet studenter og kandidater ved utdanninger innen IKT-sikkerhet de siste 5 årene. Formålet med dette avsnittet er å se nærmere på tilbudssiden, det vil si å se på hvor mange som faktisk er i gang med og fullfører utdanninger innen IKT-sikkerhet, og hvordan disse tallene har utviklet seg i løpet av de siste 5 årene.

Analysens utgangspunkt er en oversikt over tilgang på adekvat IKT-sikkerhetskompetanse, høyere utdanning/spesialistkompetanse altså på minimum bachelornivå[4]. Vi antar dermed at IKT-sikkerhetskompetanse omfatter kompetanse på minimum bachelornivå. En slik antagelse er en forenkling, siden vi med dette ikke inkluderer etter- og videreutdanning eller kompetanser oppnådd gjennom arbeidslivet eller selvlært kompetanse. Fordelen med en slik avgrensning av IKT-sikkerhetskompetanse er at det gir oss mulighet til å utnytte eksisterende statistikk og oversikter over IKT-sikkerhetsutdanninger.

Overordnet finnes det to typer IKT-sikkerhetsutdanninger. Den ene typen har IKT-sikkerhet som omdreiningspunkt, der hele utdanningen direkte eller indirekte knytter seg til IKT-sikkerhet (IKT-sikkerhetsspesialister). Den andre typen består av IKT-sikkerhetsfag som tilbys på kurs som valgfritt eller enkeltfag (IKT-sikkerhetsgeneralister). I dette avsnittet vil vi også gi en kort beskrivelse av utvalgte utdanninger og hvordan IKT-sikkerhetsutdanningene er sammensatt.

3.1 Flere studenter og kandidater

Vi presenterer her en oversikt over utviklingen i antall studenter og kandidater innen studier som gir kompetanse i IKT-sikkerhet, på bachelorgradsnivå og mastergradsnivå, i perioden 2012–2016, på basis av tall hentet fra DBH.

Tallene viser både antall «spesialister», som omfatter studieprogram spesielt innrettet mot IKT-sikkerhet, og antall «IKT-generalister», som omfatter øvrige IKT-studier med enkeltkurs i IKT-sikkerhet. De aktuelle studiene er plukket ut på basis av studieprogramnavn og emneoversikt i DBH. «Spesialist»-studiene har vi definert som studier som har sikkerhet eller security i studieprogramnavnet, mens «generalist»-studiene omfatter øvrige IKT-studier med enkeltkurs forbundet med sikkerhet/sikring/security, kryptografi/kryptologi eller «intrusion detection». I sistnevnte tilfelle har vi også supplert med opplysninger fra lærestedenes hjemmesider.

[4] Fagskoler tilbyr også kurs i IKT-sikkerhet. Ifølge DBH var det i 2017 249 studenter på kurs som hadde IKT-sikkerhet i navnet.

Denne fremgangsmåten fanger neppe oppe alle relevante studier; IKT-sikkerhet vil sikkert være en del av innholdet også i andre kurs, men vi må kunne anta at oversikten inkluderer de viktigste studiene på dette feltet.

Tallet på studenter er antall registrerte studenter i høstsemesteret. Antall kandidater er antall personer som har fullført en gradsgivende utdanning i løpet av året, både vår- og høstsemester. Vi har også sett på andel utenlandsstudenter, fordi mange utenlandsstudenter forlater Norge etter at de er ferdig med studiene. I en undersøkelse av DAMVAD (2013) fant man at dette gjaldt over halvparten av de utenlandske studentene. Utenlandske studenter er i DBH definert som studenter ved universiteter og høgskoler i Norge med utenlandsk statsborgerskap. I 2016 gjaldt dette nesten 10 prosent av studentene.

Læresteder som har blitt fusjonert inn i andre læresteder i løpet av perioden 2012–2016, har vi regnet til den institusjonen de var en del av i 2016, i hele perioden. Tallene for NTNU omfatter altså for eksempel Høgskolen i Gjøvik og Høgskolen i Sør-Trøndelag i hele perioden.

Studieprogram spesielt innrettet mot IKT-sikkerhet

Per i dag finner vi to institusjoner som tilbyr studieprogram spesielt innrettet mot IKT-sikkerhet; NTNU og Universitetet i Bergen. Ved NTNU, hvor det er et eget institutt for IKT-sikkerhet, «Institutt for informasjonssikkerhet og kommunikasjonsteknologi», er det to bachelorgradsstudier, fire mastergradsstudier og dessuten et doktorgradsstudium (ikke inkludert i student- og kandidattallene). Ved Universitetet i Bergen er det et bachelorgradsstudium.

Studieprogrammet ved Universitetet i Bergen ble introdusert i 2015. Tabell 1 viser at det i 2015 var 18 studenter og at tallet økte til 47 studenter i 2016. NTNU introduserte også et nytt bachelorstudium i 2016 med et relativt høyt antall nye studenter, 79. Også ved de allerede eksisterende studiene ved NTNU har det vært en økning i antall studenter. Fra 2012 til 2016 har det derfor vært en sterk økning i samlet antall studenter, tallet har økt med 120 prosent, fra 163 studenter i 2012 til 358 studenter i 2016. Vi forventer derfor en betydelig i økning i antall uteksaminerte kandidater de nærmeste årene, til tross for at studieprogrammet i IKT-sikkerhet ved Universitetet i Tromsø blir avviklet.

IKT-studier med kurs i IKT-sikkerhet

Videre er det 13 læresteder som tilbyr i alt 31 studieprogram med kurs i IKT-sikkerhet (inkludert valgfag); 21 på bachelorgradsnivå, 9 på mastergradsnivå og fire på doktogradsnivå. Ett av disse lærestedene har kommet til etter 2012, Nord universitet. I tillegg har det kommet til fire nye studieprogram ved de øvrige lærestedene. Antall studenter i studieprogram med kurs i IKT-sikkerhet har økt med om lag 40 prosent, fra 1 945 i 2012 til 2 736 i 2016.

Som det fremkommer av tabell 1, har NTNU også her det største studentmiljøet. Antall studenter innen disse fagene økte fra 509 i 2012 til 622 i 2016. Det nest største miljøet finnes ved Høgskolen i Bergen, der 371 personer fulgte disse fagene i 2016. Dessuten fremkommer det av tabellen at vi, med unntak av ved Universitetet i Bergen, ser en økning i antall studenter. Derfor ser vi også en betydelig økning i *samlet* antall studenter. I 2012 var det totalt 2 108 studenter innen utdanninger som helt eller delvis knytter seg til IKT-sikkerhet. I 2016 var dette tallet steget til 3 094 studenter, en stigning på 47 prosent.

Lav andel innen studieprogrammer innrettet mot IKT-sikkerhet

Sammenholdes antall studerende mellom de to lærestedene NTNU og Universitetet i Bergen, ser vi at det er en relativt lav andel studenter innen studieprogram rettet mot IKT-sikkerhet. I årene 2012–2015 ligger andelen på rundt 8 prosent, mens andelen for 2016 er økt til 11,5 prosent. Den relativt beskjedne andel kan være et problem dersom studenter som tar enkeltkurs i IKT-sikkerhet, ikke oppnår tilstrekkelig dyp kompetanse i IKT-sikkerhet til å motsvare etterspørselen og en stadig økt kompleksitet.

Tabell 1: Antall studenter på studieprogram i IKT sikkerhet og IKT-studier med kurs i IKT-sikkerhet, bachelorgrad og mastergrad. Høst-semesteret.

Lærested	2012	2013	2014	2015	2016
Studieprogram i IKT-sikkerhet					
NTNU	161	197	206	205	310
Universitetet i Bergen				18	47
Universitetet i Tromsø (avviklet)	2	1	1	1	1
Totalt	163	198	207	224	358
Studieprogram med kurs i IKT-sikkerhet					
NTNU[1]	509	594	629	647	622
Universitetet i Bergen	84	96	95	80	84
Universitetet i Oslo	210	259	297	317	359
Universitetet i Tromsø[2]	185	212	227	250	277
Universitetet i Agder	268	275	299	298	338
Universitetet i Stavanger		40	36	43	41
Nord Universitet[3]	13	18	25	52	75
Westerdals[4]	79	87	100	122	127
Høgskolen i Bergen	326	323	346	365	371
Høgskolen i Buskerud og Vestfold[5]	80	87	79	98	107
Høgskolen i Oslo og Akershus	120	114	138	152	147
Høgskolen i Telemark	31	48	48	67	83
Høgskolen i Østfold	40	69	59	88	105
Totalt	1945	2222	2378	2579	2736
Totalt	2108	2420	2585	2803	3094

Kilde: DBH og studieprogram fra lærestedenes egne hjemmesider

1) Inkludert Høgskolen i Sør-Trøndelag og Høgskolen i Gjøvik før 2016
2) Inkludert Høgskolen i Narvik før 2016
3) Inkludert Høgskolen i Nesna før 2016
4) Inkludert Norges Informasjonsteknologiske Høgskole før 2014
5) Inkludert Høgskolen i Vestfold før 2014

Tabell 2 viser antall uteksaminerte kandidater ved studieprogrammene som fremgår av tabell 1. Antallet uteksaminerte kan ikke umiddelbart sammenlignes med antall studenter, da det naturlig vil være et visst tidslag mellom antall studenter og uteksaminerte.

Av tabellen fremkommer det at antall uteksaminerte øker. For studieprogrammer spesielt innrettet mot IKT-sikkerhet øker antallet fra 25 i 2012 til 49 i 2016. Dette er en fordobling. Men som tabell 2 viser, varierer antallet. I 2015 var det 29 uteksaminerte og i 2014 51 uteksaminerte. Dette gjør det vanskelig å slå fast at vi ser en økning. Ser vi på antall studenter, tilsier det at det burde komme en økning i antall uteksaminerte. Dette vil trolig fremkomme av statistikken i 2021 og 2022.

For IKT-studier med kurs i IKT-sikkerhet er tallgrunnlaget større. Det gir et mer stabilt grunnlag å konkludere ut fra. Tabell 2 viser at antallet uteksaminerte øker fra 278 i år 2012 til 456 i år 2016, og at det er snakk om en kontinuerlig økning år for år. Sammenholdt med at antall studenter også øker år for år, se tabell 1, er det grunn til å forvente at antall kandidater vil øke de kommende årene.

Som tilfellet var med studenter, ser vi også her at andelen ferdige kandidater innen studieprogrammer rettet mot IKT-sikkerhet er lav. I 2012 var andelen 8,5 prosent, i 2014 11,5 prosent og i 2016 9,7 prosent. Den relativt lave andelen er potensielt et problem i den utstrekning enkeltkurs i IKT-sikkerhet kombinert med en bredere IKT-utdanning ikke gir tilstrekkelig kompetanse til å motsvare etterspørselen.

Tabell 2: Antall kandidater studieprogram i IKT sikkerhet og IKT-studier med kurs i IKT-sikkerhet, bachelorgrad og mastergrad. Vår- og høstsemester.

Lærested	2012	2013	2014	2015	2016
Studieprogram i IKT-sikkerhet					
NTNU	25	38	51	29	49
Universitetet i Bergen					
Universitetet i Agder	1				
Universitetet i Tromsø (avviklet)		1			
Totalt	26	39	51	29	49
Studieprogram med kurs i IKT-sikkerhet					
NTNU[1]	82	72	83	90	106
Universitetet i Bergen	16	19	17	21	21
Universitetet i Oslo	46	46	82	72	85
Universitetet i Tromsø[2]	9	20	11	25	20
Universitetet i Agder	39	53	53	60	51
Universitetet i Stavanger		8	9	11	16
Nord Universitet[3]		3	1	4	5
Westerdals	12	16	10	6	24
Høgskolen i Bergen	36	59	56	57	63
Høgskolen i Buskerud og Vestfold[4]	13	17	20	9	13
Høgskolen i Oslo og Akershus	21	24	26	21	32
Høgskolen i Telemark	4	13	9	9	7
Høgskolen i Østfold	0	0	14	18	13
Totalt	278	350	391	403	456
Totalt	304	389	442	432	505

Kilde: DBH og studieprogram fra lærestedenes egne hjemmesider

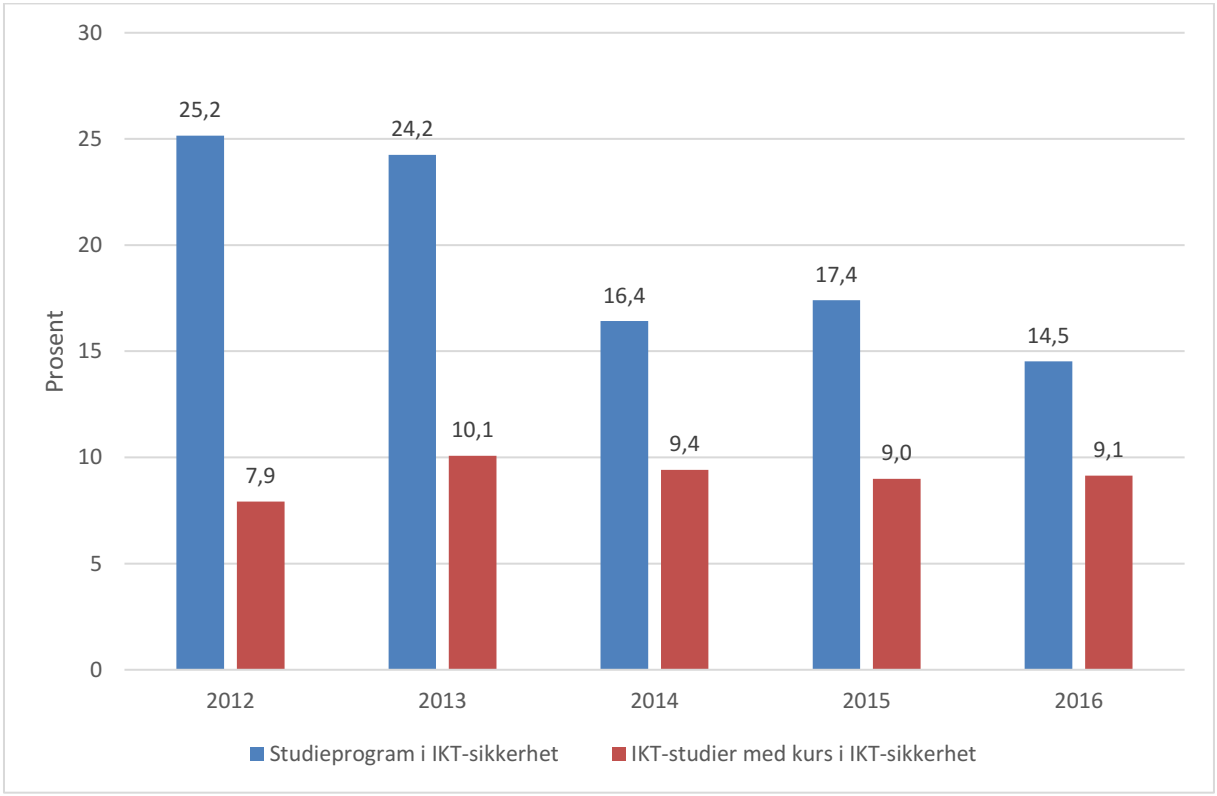
1) Inkludert Høgskolen i Sør-Trøndelag og Høgskolen i Gjøvik før 2016
2) Inkludert Høgskolen i Narvik før 2016
3) Inkludert Høgskolen i Nesna før 2016
4) Inkludert Norges Informasjonsteknologiske Høgskole før 2014
5) Inkludert Høgskolen i Vestfold før 2014

Antall utenlandske studenter

Figur 1 viser at studieprogram i IKT-sikkerhet har tiltrukket seg relativt mange utenlandske studenter, men også at andelen har sunket. I 2012 var hver fjerde student fra utlandet, hvilket tilsvarer 41 studenter. Andelen har falt jevnt over alle årene. Således var det i 2016 14,5 prosent utenlandske studenter, tilsvarende 52 studenter. Årsaken til at andelen utenlandske studenter faller, er altså ikke at det blir færre av dem, men at antallet norske studenter øker betraktelig.

Øvrige IKT-studier med kurs i IKT-sikkerhet har imidlertid ikke hatt spesielt mange utenlandske studenter, andelen har holdt seg på om lag 9 prosent i perioden vi har sett på. Det vil si at antall utenlandske studenter øker i takt med antall norske studenter. Tallene i figur 1 viser at det i 2012 var 154 utenlandske studenter, mens det i 2016 var 249 utenlandske studenter. Dette er en markant økning, men en økning som tilsvarer økningen i antallet norske studenter.

Figur 1: Antall utenlandske studenter i prosent av alle studenter. 2012–2016. Høst-semester.



Kilde: DBH og studieprogram fra lærestedenes egne hjemmesider

3.2 Innholdet i IKT-sikkerhetsutdanninger

I dette avsnittet vil vi se nærmere på innholdet i/oppbygningen av de utdanningene ved norske høyere utdanningsinstitusjoner som tilbyr kompetanse innenfor IKT-sikkerhet.

Vi vil først ta for oss de relativt få utdanningene hvor *hele* utdanningsløpet er rettet inn mot IKT-sikkerhet. Så langt NIFU har klart å bringe på det rene, dreier dette seg om 2 bachelorutdanninger (ved Universitetet i Bergen og NTNU) samt én masterutdanning og én ph.d.-utdanning, begge ved NTNU. Vi vet at en bachelorutdanning ved Universitetet i Tromsø nylig er lagt ned og at NTNU i samarbeid med en rekke andre nordiske institusjoner har hatt et tilbud om en masterutdanning, men hvor de våren 2017 ikke lenger tar opp nye studenter. Bachelorutdanningen ved NTNU er et resultat av at man valgte å slå sammen to individuelle bachelorutdanninger – sannsynligvis som en konsekvens av fusjonen mellom NTNU og blant annet Høgskolen i Gjøvik (dette har vi imidlertid ikke kontrollert). Ved NTNU tilbys også en såkalt erfaringsbasert masterutdanning innenfor IKT-sikkerhet – denne er ikke inkludert i oversikten som presenteres i dette avsnittet, i hovedsak fordi den er bygd opp av enkeltemner som i stor grad er lik den ordinære masteren.

Utvalgskriteriet for utdanningene vi har inkludert her, har vært at begrepet «sikkerhet» eller «security» (i kombinasjon med IKT/ICT) måtte gjenfinnes i utdanningens tittel.

Videre vil vi se på utdanninger hvor ett eller flere av enkeltemnene som inngår, er spesielt opprettet med tanke på IKT-sikkerhetskompetanse. Dette dreier seg om langt flere utdanninger, og innenfor rammen av dette prosjektet har det ikke vært mulig å gjennomgå alle. Vi har derfor valgt å kun inkludere de utdanningene hvor studenttallet høsten 2016 var over 100.

3.2.1 Hele utdanningsprogrammer innenfor IKT-sikkerhet

Bachelorutdanningene

Så langt NIFU har greid å identifisere, dreier altså dette seg om 2 bachelorutdanninger (våren 2017): én ved Universitetet i Bergen og én ved NTNU. Bachelorutdanningen ved Universitetet i Bergen er en bachelor innenfor informatikk, med datasikkerhet som «retning» eller spesialisering. Bachelorutdanningen ved NTNU er en utdanning innenfor IT-drift og med informasjonssikkerhet som spesialisering (se tabell 3).

En bachelorutdanning tilsvarer 180 studiepoeng, normalt 60 studiepoeng per år over en 3-årsperiode. For mange utdanningsprogram finnes det opplegg for å kunne gjennomføre utdanninger som deltidsstudent.

Tabell 3: Oversikt bachelorutdanninger innen IKT-sikkerhet; emner og antall studiepoeng

Bachelor i informatikk: Datasikkerhet UIB	Studiepoeng per semester	Bachelor i IT-drift og informasjonssikkerhet NTNU	Studiepoeng per semester
Grunnkurs i programmering (Programmering 1)	10	Grunnleggende programmering	10
Videregående programmering (Programmering 2)	10	Matematikk for informatikkfag	10
Datanett	10	Innføring i IT-drift og informasjonssikkerhet	10
Diskrete strukturar	10	Objektorientert programmering	10
Algoritmar, datastrukturar og programmering	10	Systemutvikling	10
Tryggleik i distribuerte system	10	Datanettverk	10
Informasjons-teori	10	Algoritmiske metoder	10
Lineær algebra	10	Datamodellering og database-systemer	10
Multiprogram-mering	10	Nettverks-sikkerhet	10
Programvare-sikkerhet	10	Operativ-systemer	10
Grunnleggjande koder	10	Drift av tjeneste-arkitekturer	10
Brukarkurs i matematikk I (V)	10	ITSM, risikohåndtering og sikkerhetsledelse	10
Grunnkurs i matematikk I (V)	10	Hacking, forsvar og forensics	10
System-konstruksjon (V)	10	Programvare-sikkerhet (V)	10
Modellering og optimering (V)	10	Programmerbar infrastruktur (V)	10
Algoritmer (V)	10	Applikasjons-utvikling (V)	10
Algoritme-engineering (V)	10	Økonomistyring (V)	10
Grafbasert kodeteori (V)	10	Cloud Technologies (V)	10
Informasjonsnettverk (V)	10	Ruting og svitsjing (V)	10
Kryptologi (V)	10	WWW-Teknologi (V)	10
Dataorientert visuell berekning (V)	10	Ledelse med arbeidslivsjuss (V)	10
Lineær programmering (V)	10		
Algebra (V)	10		
Diskret matematikk (V)	10		
Grunnkurs i statistikk (V)	10		

Kilde: Institusjonenes nettsider og DBH

Tabell 3 gir altså en oversikt over hvilke enkeltemner de to bachelorutdanningene (inkludert her) består av. Som nevnt skal en utdanning på bachelornivå utgjøre 180 studiepoeng (til sammen). I tabellen over er flere av emnene markert med (V), noe som innebærer at dette er et såkalt valgbart emne. De øvrige emnene er obligatoriske. De obligatoriske emnene utgjør til sammen under 180 studiepoeng, og dermed må man legge til relevante og aktuelle valgbare emner. På denne måten kan også kandidaten «spisse» sin utdanning i den retningen hun eller han syns er mest interessant.

Bachelorgraden som tilbys ved Universitetet i Bergen inneholder langt flere valgbare emner enn hva tilfellet er for utdanningen som tilbys ved NTNU. Det er selvfølgelig viktig å presisere at disse to utdanningene ikke er «like», og det er heller ikke utdanninger som forholder seg til en overordnet felles rammeplan som til dels styrer innholdet i studiet, slik tilfellet er for andre typer utdanninger (for eksempel innen helse, økonomi og administrasjon, lærere).

Universitetet i Bergen presenterer den aktuelle bachelorutdanningen slik: «Bachelorstudiet i datatryggleik tek opp korleis ein kan utforme, implementere og analysere IKT-infrastruktur som er robust mot både tilfeldige feil og målretta angrep. Målet med programmet er å gi både ei teoretisk forståing for robuste IKT-system, og ei praktisk evne til å utvikle og halde ved like slike system.»

På NTNUs nettsider står følgende å lese om bachelorutdanningen i IT-drift og informasjonssikkerhet: «Studiet gir en grunnleggende informatikkutdannelse, men med større vekt på drift og sikkerhet enn det som er vanlig i slike studier. IT-drift og informasjonssikkerhet bygger på en solid grunnleggende forståelse av datasystemer.»

Både introduksjonen på lærestedenes nettsider og innholdet i selve utdanningen (slik det er presentert i tabell 3) tilsier at dette er to utdanninger som gir omfattende kompetanse innen IKT-sikkerhet, men med ulik tilnærming. Begge utdanningene har kunnskap om programmering som utgangspunkt, men mens Universitetet i Bergen har en mer generell og teoretisk tilnærming, ser det ut som om NTNU har en mer praktisk tilnærming. Universitetet i Bergen ønsker å utdanne kandidater som vil gå videre og ta masterutdanning, mens dette ikke er et uttalt mål for kandidatene ved NTNU. Dette kan kanskje også ha noe å gjøre med de to ulike lærestedenes profil. NTNU utdanner kandidater som kan drifte et IT-system på en sikker måte, mens man ved Universitetet i Bergen er mer opptatt av informasjonssikkerhet på et mer overordnet nivå.

Det er kanskje verdt å legge merke til at hvert enkeltemne skal utgjøre 10 studiepoeng. I ett semester skal det normalt inngå 30 studiepoeng.

Masterutdanning

Tabell 4 gir en oversikt over enkeltemnene i den masterutdanningen i IKT-sikkerhet (som også heter Master in Information Security) vi har tatt med i dette avsnittet. Undervisningen foregår på engelsk, og enkeltemnene er derfor gjengitt på engelsk i tabellen. Dette er en såkalt toårig masterutdanning, det vil si at den bygger på andre utdanninger på et lavere nivå. Dette kan for eksempel være bachelorutdanningen beskrevet over i tabell 3 eller andre bachelorutdanninger innen informatikk, programvareutvikling, informasjonssystemer, informasjonsteknologi, datateknikk eller tilsvarende. Dersom man velger dette studiet, vil man måtte velge mellom tre ulike spesialiseringer:

- Cyber and Information Security Technology
- Information Security Management
- Digital forensics

Tabell 4: Masterutdanningen innen IKT-sikkerhet ved NTNU, enkeltemner og studiepoeng

Cyber and Information Security Technology	Studiepoeng per semester	Information Security Management	Studiepoeng per semester	Digital Forensics	Studiepoeng per semester
Introduction to Cyber and Information Security Technology	7,5	Scientific Methodology and Communication	7,5	Scientific Methodology and Communication	7,5
Introduction Digital Forensics	7,5	Introduction to Cyber and Information Security Technology	7,5	Introduction to Information Security Management	7,5
Introduction to Information Security Management	7,5	Introduction Digital Forensics	7,5	Introduction Digital Forensics	7,5
Scientific Methodology and Communication	7,5	Introduction to Information Security Management	7,5	Introduction to Cyber and Information Security Technology	7,5
System Security	7,5	Security Management Metrics	7,5	Cybercrime Investigation	7,5
Cryptology	7,5	Socio-technical Systems Enabled Crime	7,5	Data Science for Security and Forensics	7,5
Network Security	7,5	Risk Management for Information Security	7,5	System Security	7,5
Biometrics	7,5	Elective	7,5	Network Security	7,5
Critical Infrastructure Security	7,5	Theory and Practise of Legal, Privacy, and Organizational Requirements	7,5	Intrusion Detection in Physical and Virtual Networks	7,5
Intrusion Detection in Physical and Virtual Networks	7,5	Security Privacy and Risk Management Case Study	7,5	Computational Forensics	7,5
Research Project Planning	7,5	Research Project Planning	7,5	Research Project Planning	7,5
Elective	7,5	Elective	7,5	Elective	7,5
Master's Thesis	30	Master's Thesis	30	Master's Thesis	30

Kilde: Institusjonenes nettsider og DBH

På NTNUs nettsider er masterutdanningen beskrevet på følgende måte: «Studiet skal gi deg ferdigheter som gjør deg i stand til å planlegge, gjennomføre og lede arbeid innen informasjonssikkerhetsfaget i både offentlig og privat sektor på en profesjonell måte. Informasjonssikkerhet er et tverrfaglig område, og krever en solid basis i informatikk og matematikk.»

På NTNUs nettsider er masterutdanningen beskrevet på følgende måte: «Studiet skal gi deg ferdigheter som gjør deg i stand til å planlegge, gjennomføre og lede arbeid innen informasjonssikkerhetsfaget i både offentlig og privat sektor på en profesjonell måte. Informasjonssikkerhet er et tverrfaglig område, og krever en solid basis i informatikk og matematikk.»

Videre heter det i beskrivelsen av studiet at kandidaten skal ha «kunnskaper og ferdigheter om relevante teknologiske, samfunnsmessige og rettslige aspekter ved faget informasjonssikkerhet.» Som tabellen viser vil en mastergrad bestå av mange enkeltemner, og masteroppgaven utgjør hoveddelen eller tyngdepunktet i utdanningen. Enkeltemnene er i all hovedsak obligatoriske, og hvert emne utgjør kun 7,5 studiepoeng – noe som selvfølgelig begrenser hvor dypt i materien man har anledning til å gå innen hvert emne. Dermed blir det masteroppgaven og problemstillingen kandidaten velger for denne som får størst betydning for hva kandidaten kan mest om etter endt utdanning. Imidlertid skal jo også retningen/spesialiseringen som studenten velger for hele masterløpet sitt, være en god indikasjon på hvilken kompetanse den enkelte kandidat har.

Tabell 5 gir en oversikt over obligatoriske og valgbare enkeltemner som inngår i ph.d.-utdanningen i IKT-sikkerhet (Information security) som tilbys ved NTNU. Ph.d.-utdanningen skal til sammen i løpet av 3 år utgjøre 180 studiepoeng. Av disse 180 studiepoengene er det avhandlingen som gir de aller fleste, men det anbefales at studentene tar minst 30 studiepoeng i tillegg til arbeidet med avhandlingen. For ph.d.-programmet Information security er to av enkeltemnene listet i tabellen under obligatoriske. Dette er:

- Ethics and Legal Aspects of Scientific Research
- Introduction to Information Security

I tillegg bør så studenten inkludere ett til to valgbare emner i graden. Innholdet i en utdanning på ph.d.-nivå vil i stor grad være basert på den enkeltes ønsker og interesser – innenfor det aktuelle overordnede tema.

Tabell 5: Ph.d.-utdanningen i IKT-sikkerhet ved NTNU, enkeltemner og studiepoeng

PhD programme in Information Security	Studiepoeng per semester (semester 1 + 2)
Introduction to Information Security (O)	5 + 5
Ethics and Legal Aspects of Scientific Research (O)	5 + 5
Foundations of Information Security (V)	5
Intrusion Detection and Prevention (V)	5
Selected Topics in Cryptology (V)	5
Wireless Communication Security (V)	5
Biometrics (V)	5
Modern Cryptology (V)	5 + 5
Computational Forensics (V)	5
Computational Intelligence (V)	5
Risk Management I (V)	5
Behavioural Biometrics (V)	5 + 5
Computational Image Processing (V)	5 + 5
Selected topics in Colour Imaging (V)	5 + 5
Selected topics in Image Processing (V)	5 + 5
Selected Topics in Video Processing (V)	5 + 5
Real-time AI for robotics and simulated environments (V)	5
Selected Topics in Database Systems (V)	5
Selected Topics in Web-Based Systems (V)	5
Colour Science (V)	5 + 5
Image Quality (V)	5 + 5
Mobile Technology (V)	5 + 5
Serious Games (V)	5
Quality in Academic Research (V)	5 + 5
Scientific Communication (V)	5 + 5
Critical Thinking (V)	5 + 5
Risk Management II (V)	5
COINS Winter School (V)	3
COINS Summer School (V)	3
COINS Workshop (V)	1

Kilde: Institusjonenes nettsider og DBH

En ph.d.-grad er en forskerutdanning, og denne skal bidra til at kandidaten er i stand til å utøve forskning innenfor gjeldende standarder og retningslinjer på sitt fagfelt. Noe av det viktigste forskerutdanningen skal bidra til å utvikle er kandidatens evne til å identifisere nye problemer/utfordringer innen fagfeltet, for at hun/han så skal kunne vurdere hvilken innvirkning disse vil kunne ha på samfunnet for øvrig. Innenfor et fagfelt som IKT representerer, kan man anta at evne til raskt å identifisere nye problemer og samtidig kunne vurdere innvirkning og igangsette tiltak, eventuelt ny forskning, vil være av meget stor viktighet både nå og i fremtiden.

3.2.2 Studier med enkeltfag innen IKT-sikkerhet

Det er selvfølgelig en rekke utdanninger på alle nivåer som inneholder elementer av IKT-sikkerhet, men hvor ikke hele studiet er viet akkurat dette feltet. Dette dreier seg om utdanninger innen data og informasjonsteknologi som ofte er del av en ingeniørutdanning.

I oversikten under (tabell 6 og tabell 7) er det kun enkeltemner ved de største (over 100 studenter) utdanningsprogrammene som er inkludert. Oversikten er fordelt etter lærested og nivå på. utdanningen.

Tabell 6: Oversikt over utdanninger ved universitetene som inneholder enkeltemner innenfor IKT-sikkerhet

Lærested, Universitetene	2016 Antall studenter	Enkeltemner innenfor IKT-sikkerhet
NTNU		
Bachelor i ingeniørfag - data	117	*Informasjonssikkerhet*, høst 3.år, 10 sp., valgbart
Bachelor i informatikk med spesialisering i informasjonsbehandling - 654121	127	*Informasjonssikkerhet og produktforvaltning*, vår 2.år, 15 sp., obligatorisk
Kommunikasjonsteknologi – masterstudium (5-årig) – 754109, (Valg av hovedprofil i 4.årskurs – Informasjonssikkerhet er en av tre valgmuligheter)	209	*Sikkerhet og robusthet i IKT system*, høst 2.år, 7,5 sp., obligatorisk; *Informasjonssikkerhet*, vår 3.år, 7,5 sp., obligatorisk; *Informasjonssikkerhet i trådløse nett*, høst 4.år, 7,5 sp., obligatorisk; *Risikohåndtering, samfunnssikkerhet og beredskap*, høst 4.år, 7,5 sp., valgbart; Etisk hacking - *Informasjonssikkerhet, fordypningsemne*, høst 5. år, 7,5 sp., obligatorisk; *Introduction to Information Security Management*, høst 5. år, 7,5 sp., valgbart; *Risikohåndtering, samfunnssikkerhet og beredskap*, høst 5.år, 7,5 sp., valgbart
Universitetet i Oslo		
Informatikk: programmering og nettverk (master – to år), Informasjonssikkerhet er én av fire mulige spesialiseringer	306	Relevante emner for informasjonssikkerhet: *Innføring i kryptografi*, *Sikkerhet i operativsystemer og programvare*, *Informasjonssikkerhet i industrielle sensor og mobile systemer*, *Uangripelige IT-systemer* (høstemner); *Formell modellering og analyse av kommuniserende systemer*, *Logikk for systemanalyse (PMA)*, *Sikkerhet i distribuerte systemer* (våremner)
Ingeniørfag – data, bachelorprogram, i 3.semester kan man velge å bl.a. spesialisere seg innenfor nettverksdrift og sikkerhet	252	*Nettverk og sikkerhet*, 4.sem., 10 sp., obligatorisk; *Scripting og hacking*, 5.sem., 30 sp., valgbart

Kilde: Institusjonenes nettsider og DBH

Oversikten i tabell 6 og 7 gir noe informasjon om hvilken tematikk innenfor IKT-sikkerhet de ulike utdanningene anser som mest interessant og relevant. Også ved å se på hvorvidt enkeltemnet er obligatorisk eller valgbart og hvor mange studiepoeng som inngår, vil man få en indikasjon på hvor viktig kompetanse i IKT-sikkerhet blir ansett å være for den aktuelle utdanningen.

Tabell 7: Oversikt over utdanninger ved *høgskolene* som inneholder enkeltemner innen IKT-sikkerhet

Lærested, Høgskolene	2016 Antall studenter	Enkeltemner innenfor IKT-sikkerhet
Westerdals		
Bachelor - programmering	127	Informasjonssikkerhet, 2.sem., 7,5 sp., obligatorisk
Høgskulen på Vestlandet (Høgskolen i Bergen)		
Data (bachelor 3-årig), *Drift av datasystemer* (en av tre spesialiseringer)	184	Nettverksadministrasjon, drift og sikkerhet, 5.sem., 10 sp., obligatorisk (dette emnet kan inngå som valgbart i de andre spesialiseringene)
Høgskolen Sør Øst Norge (Høgskolen i Buskerud og Vestfold)		
Bachelor i ingeniørfag, datateknikk 654122 (spesialisering innen bl.a. sikkerhet – cyber security)	107	
Høgskolen i Oslo og Akershus		
Bachelorstudium i informasjonsteknologi 654120	147	Datasikkerhet, 5.sem., 10 sp., obligatorisk
Høgskolen i Østfold		
Bachelorstudium i informatikk – design og utvikling av IT-systemer 654121	105	Innføring i datasikkerhet, 2.sem., 10 sp., obligatorisk

Kilde: Institusjonenes nettsider og DBH

4 Mangel på IKT-sikkerhetskompetanse i fremtiden

I analysen opererer vi med IKT-sikkerhetskompetanse på avansert nivå. Det vil si kompetanse på minimum bachelornivå. For å identifisere hvilke utdanninger det er tale om, har vi systematisk gjennomgått utdanningsprogrammer i Database for statistikk om høgre utdanning (DBH). Her har vi identifisert utdanninger på minimum bachelornivå, der IKT-sikkerhet er grunnlag for hele utdanningen eller er en del av utdanningen. Eksempler på disse utdanningene er:

- Bachelor i IT-drift og informasjonssikkerhet ved NTNU, hvor det bl.a. undervises i:
  - Nettverkssikkerhet
  - ITSM, risikohåndtering og sikkerhetsledelse
  - Hacking, forsvar og forensics
  - Ledelse med arbeidslivsjuss
- Master 2-årig Informatikk: programmering og nettverk ved UiO hvor det bl.a. undervises i:
  - Innføring i kryptografi
  - Sikkerhet i operativsystemer og programvare
  - Informasjonssikkerhet i industrielle sensor og mobile systemer

Ved hjelp av statistikk basert på registre hos SSB kan vi se hvor personer med disse utdanninger blir ansatt. Da har vi informasjon om utdanning og arbeidsmarkedstilknytning. Dette er informasjoner som vi anvender som grunnlag for våre fremskrivninger. I det følgende presenteres innledende betraktninger av næringen IKT-sikkerhet. Dernest gis en introduksjon til framskrivningsmodellene før resultatene presenteres..

4.1 Næringen for IKT-sikkerhet

Der finnes per i dag ingen statistikk som gir en samlet oversikt over IKT-sikkerhetsnæringen. Det skyldes at IKT og IKT-sikkerhet går på tvers av eksisterende sektorer og næringsgrupperinger. Således finnes foretak som arbeider med IKT-sikkerhet innen industrien, detaljhandel, vitenskapelig tjenesteyting, offentlig sektor og selvsagt også innen IKT-næringen. Det er således vanskelig å få full oversikt over næringen IKT-sikkerhet, som den ser ut per i dag.

Basert på en gjennomgang av oversikter[5] har vi søkt å sammenfatte en mulig oversikt over IKT-sikkerhetsnæringen. Vår sammenstilling klarer å identifisere foretak som helt eller delvis opererer

[5] Se følgende oversikter: 1)http://www.norwayexports.no/sectors/, 2)http://www.largestcompanies.com/toplists/norway/largest-companies-by-turnover/industry/security-and-investigation-

innen IKT-sikkerhet. Disse foretakene har til sammen 9 249 sysselsatte. Tallet må ses som et estimat på størrelsen på IKT-sikkerhetsnæringen. For det første har vår kartlegging langt fra avdekket samtlige foretak som jobber helt eller delvis med IKT-sikkerhet, eksempelvis innen finansnæringen. Selv om vi har med enkelte foretak fra offentlig sektor, er det gitt at vi ikke dekker hele offentlig sektor inklusiv både helse og omsorg, etater samt militære og annen samfunnssikkerhet. Det tilsier at estimatet er betydelig undervurdert. Samtidig vil ikke alle sysselsatte som jobber i foretakene som er identifisert i vår analyse, jobbe med IKT-sikkerhet, hvilket vil tilsi at anslaget på 9 249 sysselsatte er et overestimat.

Gjennomgangen har gitt oss innblikk i hvilke områder disse foretakene befinner seg innenfor. Eksempler på hvilke områder personer med IKT-sikkerhetskompetanse arbeider innenfor er:

- CCTV, IP-nettverksløsninger
- Produksjon av medisinsk utstyr
- Instrumenteringssystemer, overvåkingssystemer og kontrollsystemer
- Satellitter, fly og militære våpen

Den overordnede IKT-næringen sysselsetter rundt 100 000, viser Menon Business Economics (Maurseth, Holmen, & Løge, 2015) i en rapport gjennomført for IKT-Norge. De avgrenser den norske IKT-næringen ut fra fire kjernebransjer:

- Telekom
- Generelle programvarer
- Skreddersydde IT-tjenester
- IKT-driftstjenester
- I tillegg to støttebransjer: IKT-industri og IKT-handel.

Et sentralt omdreiningspunkt for rapporten er at standardiserte næringskoder (såkalte NACE-koder) ikke kan anvendes til å avgrense IKT-næringen, da den går på tvers av eksisterende sektorer og næringer. Dersom vi følger standardiserte næringskoder, så viser Statistisk Sentralbyrå at det i 2016 var 97 000 sysselsatte i det som under en samlet betegnelse kalles «Informasjon og kommunikasjon», og som dekker:

- NACE 58: Forlagsvirksomhet
- NACE 59: Film, video og fjernsynsproduksjon, utgivelse av musikk- og lydopptak
- NACE 60: Radio- og fjernsynskringkasting
- NACE 61: Telekommunikasjon
- NACE 62: Tjenester knyttet til telekommunikasjon
- NACE 63: Informasjonstjenester

Selv om flere av disse i tradisjonell forstand ikke inneholder et teknologielement, så har de seneste års utvikling ført til at disse næringene i dag i stor grad bygger på teknologi. Derfor gir det mening å tilføye teknologi til betegnelsen «Informasjon og kommunikasjon», som således blir til IKT.

Vår oppdeling for de 9 249 sysselsatte lar seg ikke direkte sammenligne med de øvrige oppdelingene. Dertil er vår oppdeling basert på et for tynt grunnlag. Om det skal utarbeides en faktisk opptelling av IKT-sikkerhetsnæringen, vil dette kreve et eget prosjekt.

activities, 3) https://www.sourcesecurity.com/companies/search-results/company-search/c.norway,t.systems-integrators.html, 4) http://www.cybersecuritycareers.net/NO/#jobresults

4.2 Introduksjon til framskrivningene, MODAG og MOSART

Framskrivning av tilbud og etterspørsel etter personell med IKT-sikkerhetskompetanse følger samme fremgangsmåte som lignende studier av fremtidens tilbud og etterspørsel etter arbeidskraft, se Bjørnstad (2010), Cappelen (2013), DAMVAD (2014) og Dapi (2016). I likhet med disse studiene anvendes MODAG og MOSART til å fremskrive tilbud og etterspørsel.

Framskrivning av etterspørselssiden drives av makromodellen MODAG. MODAG er en modell for norsk økonomi utviklet av Statistisk sentralbyrå (SSB). Modellen er estimert på årlige nasjonalregnskapsdata og gir detaljert viten om hvordan norsk økonomi utvikler seg. Derfor anvendes MODAG til framskrivninger og politikkanalyser på kort og mellomlang sikt. Finansdepartementet er hovedbruker av MODAG. MODAGs detaljrikdom gjør den egnet til detaljerte analyser. Modellen tar høyde for særtrekk ved den norske økonomien, som oljesektoren og en sentralisert lønnsdannelse med lønnsforhandlinger mellom arbeidsgiver- og arbeidstakerorganisasjoner, hvilket gjør modellen velegnet til å analysere den norske økonomien.

MOSART anvendes til å fremskrive tilbudssiden. Modellen brukes til en rekke formål, blant annet til framskrivninger av pensjoner og befolkningens utdanningsnivå. MOSART benytter individuelle kjennetegn for det enkelte individ, og på bakgrunn av dette beregnes sannsynlige valg knyttet til utdanning og arbeidsmarkedstilknytning. År for år estimeres sannsynligheten for at et individ med kjente kjennetegn, basert på blant annet kjønn og alder, starter en utdanning, valg av utdanningsnivå og -retning og om hun/han fullfører utdanningen. Dette beregnes for i alt 29 utdanningsgrupper.

For å beregne tilbud og etterspørsel etter IKT-sikkerhetskompetanse har vi estimert andelen en gitt utdanningsgruppe og næring har av en av de utdanningene, som vi har identifisert i kapittel 2. Ved å holde disse andelene fast over tid, frem til år 2030, kan vi estimere etterspørsel (MODAG) og tilbud (MOSART). For noen næringer og utdanningsgrupper vil andelen være 0 prosent, mens for andre vil det være tale om en betydelig andel. Ved å holde andelen fast oppnås resultatene av framskrivningen som vises i appendiks kapittel 4.4, noe som kan kalles basisframskrivning. I appendiks finnes likeledes en mer utførlig beskrivelse av MOSART og MODAG.

Fordelene ved å benytte MODAG og MOSART er detaljeringsgraden og muligheten til å gå inn og gjøre kvalitative endringer. Eksempelvis bygger hovedresultatet fra denne studien på kvalitative justeringer av basisframskrivning. Kvalitative justeringer er gjort med utgangspunkt i nylig tilgjengelig informasjon. En hjørnestein i MODAG og MOSART er befolkningsframskrivinger. Befolkningen er noe av det mest sikre å fremskrive, da både fødselsrater, innvandring/utvandring og dødelighetsnivå holder seg relativt stabilt. Samtidig er det en styrke i MODAG at etterspørsel etter arbeidskraft er konsistent med en rekke andre faktorer i utviklingen i norsk økonomi, herunder BNP, produktivitet, eksport/import og lønnsdannelse.

Omvendt så bygger MODAG og MOSART på historiske data, hvilket gir begrensninger. De historiske dataene gir grunnlaget for beregning av de statistiske sammenhengene, som danner grunnlaget for framskrivninger. Her vil betydelige endringer de senere år ikke ha gjennomslagskraft. I kapittel 2 så vi at antallet studenter økte med nærmere 50 prosent. En slik økning må alt annet likt antas å øke antallet uteksaminerte kandidater og dermed øke tilbudssiden. Dette vil ikke MOSART fange opp.

Etterspørselen er basert på tall over faktisk sysselsetting og ikke et underliggende behov som finnes i næringslivet og offentlig sektor. Det kan være mange grunner til at faktisk sysselsetting avviker fra behovet. For eksempel kan det være ønske om å ansette flere personer med en gitt utdanning, men siden det ikke er flere i markedet, får man ikke fylt de ledige stillingene. Alternativt ansettes personer med en ikke adekvat utdanning, men som allikevel vurderes å kunne dekke den etterspurte kompetansen. MODAG vil ikke fange opp eventuelle underliggende behov.

Det finnes måter å søke å avdekke disse underliggende behovene på. Det kan foretas surveys, hvor arbeidsgivere blir bedt om å svare på om de har udekkede kompetansebehov[6]. Alternativt kan man anvende registerdata fra SSB til å se på arbeidsmarkedstilknytningen til nyutdannede innen utdanning med IKT-sikkerhet. Et annet alternativ er å se på lønnsdannelsen for gruppen med utdanning innen IKT-sikkerhet. Selv om det er sentral lønnsdannelse i Norge, kan det godt være individuelle forskjeller som kan avspeile en ubalanse mellom tilbud og etterspørsel.

En mulig utfordring ved framskrivningen er at populasjonen av personell med IKT-sikkerhetskompetanse er relativt liten i utgangspunktet; den består av under 10 000 personer. Detaljeringsgraden i MODAG og MOSART gjør at modellene godt kan håndtere mindre populasjoner, for eksempel fremskriver Bjørnstad m.fl. (2010) og DAMVAD (2014) med utgangspunkt i populasjoner på under 10 000 personer. En liten populasjon vil dog alt annet likt være mer følsom overfor endringer. Det kan eksempelvis være endringer i antall studenter, som vi tidligere har nevnt, eller markante endringer i etterspørsel som følge av endret trusselbilde. I utgangspunktet må framskrivninger anses som et estimat med en viss usikkerhet. En mindre populasjon vil øke denne usikkerheten.

4.3 I år 2030 vil 4 100 stillinger innen IKT-sikkerhet være ubesatt

I dette avsnittet presenteres resultatet av framskrivningen av fremtidens mangel på IKT-sikkerhetskompetanse. Resultatene følger av en kvalitativ justering av basisscenarioet, som presenteres i appendiks. Basisscenarioet bygger på det vi kan kalle basisframskrivninger. Her gjøres ingen endringer i forhold til vårt utgangspunkt for framskrivning. Det vil si at vi anvender de tallene som vi finner frem til gjennom den statistiske kartleggingen i DBH, AA-registre, BHU-register samt konvertering av disse til MOSART og MODAG[7].

Dette er en studie som hovedsakelig baserer seg på et kvantitativt datagrunnlag, og resultatene må betraktes som foreløpige. Det er kvalitative forhold som er helt eller delvis fraværende, da de krever en grundig gjennomgang, herunder vurdering av gjennomslag på framskrivning. Dette gjelder for eksempel på tilbudssiden, der det åpnes opp for enda flere studieplasser til de mange som søker utdanninger med IKT-sikkerhetsinnhold. Men det gjelder også på etterspørselssiden, for eksempel der IKT-sikkerhetskompetanse vil bli enda mer etterspurt enn det vi ser i dag. Begge deler anser vi som sannsynlige, men vi har ikke mulighet per nå til å fastslå gjennomslag på framskrivninger.

Vi har inkludert alle identifiserte studier som har fag innen IKT-sikkerhet, jf. gjennomgang i kapittel 2. Dette betyr at vi har tatt med studier som har begrenset faglig innhold rettet mot IKT-sikkerhet. Dette skulle tilsi at vi potensielt overestimerer resultatene, både på tilbuds- og etterspørselssiden.

Omvendt vil fag innen generell IKT-kompetanse inneholde undervisning i IKT-sikkerhet. Det er vanskelig å se for seg fag ved oppbygging av IT-infrastruktur, nettverksløsninger og cloud-teknologi som ikke inneholder et aspekt av IKT-sikkerhet. Dermed kan disse kandidatene være aktuelle for jobber innen IKT-sikkerhet. Dette vil på sin side tilsi en underestimering av resultatene både på tilbuds- og etterspørselssiden.

Når det gjelder de framskrivningsmodellene som er anvendt, er det foretatt følgende kvalitative justeringer:

- IKT Norge har i 2015 anslått at det manglet mellom 6 300 og 8 600 kandidater med IKT-kompetanse i Norge, IKT-Norge (2015). I denne studien har vi justert tilbudssiden med rundt en tredjedel av de 6 300 kandidatene i år 2015. Vi justerer tilbudssiden fordi vi ser at enkelte av de utdanningene vi har inkludert har IKT-sikkerhet som en begrenset del av utdanningen, eksempelvis 7,5 til 10 studiepoeng innenfor en 2- eller 3-årig utdanning. Dermed er det

[6] Se eksempelvis IKT-Norge (2015) «Kritisk mangel på IKT-kompetanse», eller alternativt NAVs bedriftsundersøkelse.
[7] Denne fremgangsmåten er identisk med og bygger på metoden som anvendes i rapporten «Dimensjonering av avansert IKT-kompetanse», DAMVAD og Samfunnsøkonomisk analyse (2014)

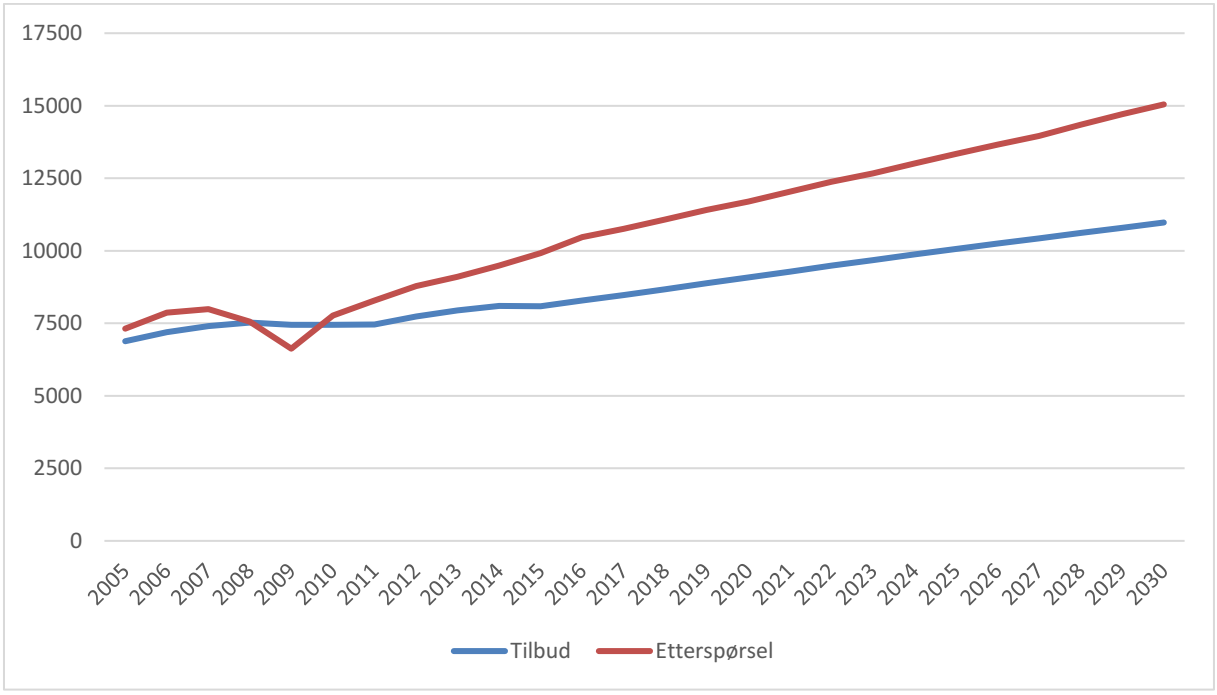
usikkert om disse utdanningene gir kandidatene den ønskede og etterspurte kompetansen. Vi har derfor valgt å nedjustere tilbudssiden fremfor å oppjustere etterspørselssiden.

- Nedjustering av tilbudssiden inngår i framskrivningen frem mot år 2030. Det betyr at tilbudssiden nedjusteres med rundt 2 000 personer fra år 2015 og frem til 2030, mens vi gradvis nedtoner betydning av nedjusteringen tilbake i tid slik at tilbudssiden i år 2005 nedjusteres med rundt 600 personer.
- Omvendt oppjusteres tilbudssiden fra år 2016 og fremover. Det er snakk om oppjustering som søker å motsvare de økningene vi ser fra opptak og uteksaminerte i NSDs Database for statistikk om høyere utdanning. Oppjusteringen betyr at det i år 2030 er rundt 1 000 flere utdannet innenfor IKT.

Vi finner i våre framskrivninger at det vil være en mismatch mellom tilbud og etterspørsel på rundt 4 100 personer i år 2030. I år 2030 vil det på tilbudssiden være 10 974 personer som har IKT-sikkerhetskompetanse på minimum bachelornivå. Samme år vil etterspørselen være på 15 045 personer. Figur 2 viser framskrivningen.

Figuren viser at til tross for en forventet stabil økning av personer med IKT-sikkerhetskompetanse, øker gapet. Det skyldes en enda kraftigere økning i etterspørselen. I år 2030 passerer etterspørselen 15 000 personer. Dette svarer til at tilbudssiden må øke med godt og vel en tredjedel for å kunne møte fremtidens etterspørsel.

Figur 2: Tilbud og etterspørsel etter personell med IKT-sikkerhetskompetanse



Kilde: NIFU 2017

Tallene viser et fall i etterspørselen i år 2008 og 2009. Dette er konsekvensen av finanskrisen i annen halvdel av år 2000. Krisen begynte for alvor i år 2008 og kulminerte i august 2008, da Lehman Brothers med over 26 000 ansatte gikk konkurs. Etterspørselen etter personer med IKT-sikkerhetskompetanse er dog så sterk at fallet i etterspørselen er utjevnet allerede i år 2011.

Vi ser av ovenstående at etterspørselen etter IKT-sikkerhetskompetanse i 2015 ligger på knapt 10 000 personer. Dette er ikke identisk med omfanget av en IKT-sikkerhetsnæring, men går på tvers av alle

næringer inklusiv offentlig sektor. For å si noe om omfanget viser vi her eksempler på andre yrker med tilsvarende antall sysselsatte[8]:

- Bussjåfører og trikkeførere, 14 061 sysselsatte
- Elektronikkingeniører, 12 180 sysselsatte
- Finans- og investeringsrådgivere, 10 440 sysselsatte
- Frisører, 9 971 sysselsatte
- Journalister, 7 233 sysselsatte

Økt fokus på IKT-sikkerhet vil øke fremtidens behov for personer med avansert IKT-kompetanse. Det viser en tidligere analyse med fokus på den generelle dimensjoneringen av framtidens behov for avansert IKT-kompetanse, DAMVAD & Samfunnsøkonomisk analyse (2014). I rapporten beskrives et scenario der: «.. Norge i år 2025 (der) *metodene for både å tilrane seg data og beskytte seg er avanserte. Samfunnet har det siste tiåret opplevd flere skandaler knyttet til misbruk av så vel pasientdata for utpressingsformål som regelrett bedriftsødeleggelse, som følge av tyveri av data. Både virksomheter og befolkning er villig til å investere betydelig med tid og penger på å beskytte tilgang til data om seg og sitt.»* Med de mange eksemplene fra kapittel 1 kan vi si at vi allerede per i dag er veldig nære ved å være i en slik situasjon som scenariet beskriver. Her pekes det på at en slik situasjon vil øke etterspørselen etter personer med avansert IKT-kompetanse med mer enn 4 000.

4.4 Oppsummerende betraktninger rundt kvantitativ framskrivning

Denne studien hadde i utgangspunktet følgende mandat: «Hovedformålet med prosjektet er forslag til tilnærming og datagrunnlag for oppdatert kunnskap om tilgangen på IKT-sikkerhetskompetanse, høyere utdanning/spesialistkompetanse, sett i forhold til arbeidslivets framtidige behov (både offentlig og privat sektor) for slik kompetanse.» Som rapporten viser, gikk studien litt videre og endte med et foreløpig estimat på fremtidens tilbud og etterspørsel.

Rapporten peker på et betydelig underskudd av fremtidig personell med rettet IKT-sikkerhetskompetanse. Tallene må selvsagt tas med forbehold. Dels er det de generelle forbeholdene om framskrivninger, der de absolutte tallene må ses som et skjønnsmessig estimat. Dels har studien hatt en naturlig begrensning med hensyn til tidsramme og allokeringen av ressurser.

Underdekningen av personer med IKT-sikkerhetskompetanse er større i år 2030 end underdekningen av personer med generell IKT-kompetanse. Tallene peker på at det i 2030 vil være en etterspørsel etter personer med IKT-sikkerhetskompetanse på rundt 15 000 og en underdekning på rundt 4 100. En lignende framskrivning pekte på at det i 2030 vil være en etterspørsel etter IKT-kompetanse generelt på 55 000 personer og en underdekning på 10 500. Etterspørselen efter personer med IKT-sikkerhetskompetanse utgjør da 27 prosent av den samlede etterspørselen etter personer med IKT-kompetanse, mens underdekningen er i underkanten av 40 prosent.

Uansett forbehold er det liten tvil om at behovet for IKT-sikkerhetskompetanse vokser. Det viser en lang rekke undersøkelser, jf. gjennomgangen i kapittel 1 i denne studien. I samme kapittel pekes det på at det er dyrt og risikabelt ikke å ha kontroll på IKT-sikkerheten. Den seneste saken om manglende kontroll på IKT-sikkerhet i Helse Sør-Øst viser at IKT-sikkerhet ikke bare handler om teknisk kompetanse, men at IKT-sikkerhet også er et sentralt ledelsesspørsmål. Rapportene fra PriceWaterhouseCoopers peker på at budsjettene for IKT-sikkerhet øker ganske betydelig de kommende år, noe som igjen vil øke etterspørselen etter IKT-sikkerhetskompetanse.

Antall studenter økte betydelig i perioden 2012–2016. Dette vil trolig bety en økning på tilbudssiden og vil understøtte økningen som har funnet sted i antall kandidater de seneste 5 år. Det sentrale

[8] Tallene bygger på SSB register basert sysselsetting oppgjort per 4.kvartal 2016.

spørsmål er da om antall kandidater øker nok til å dekke økningen i etterspørselen. Og vil de ekstra kandidatene besitte den etterspurte kompetansen?

Tallene over antall kandidater viser en betydelig økning fra 2012 til 2016. I tillegg peker tallene for antall studenter på en betydelig økning fremover. Modellene for beregning av fremtidens tilbudsside bygger på tidsserier som ikke tar med de senest observerte økningene i antall studenter. Dette kan bety at tilbudssiden vil øke mer enn modellen forespeiler.

Omvendt vil nok vår framskrivning av etterspørselssiden undervurdere fremtidens behov. I studien er det forsøkt korrigert for at det allerede per i dag er en mangel på personell med IKT-sikkerhetskompetanse. Vi vet imidlertid ikke hvor stort dette tallet er[9]. Samtidig pekes det fra mange sider på at det kommer en kraftig økning i etterspørselen etter IKT-sikkerhetspersonell, en økning som allerede kan observeres nå, men som er vanskelig å kvantifisere presist og dermed inkludere i framskrivningsmodellene.

Usikkerhetene til tross, så peker framskrivningene på at det vil være en betydelig underdekning av fremtidens behov for IKT-sikkerhetskompetanse. En mulighet for å minke underdekningen kan være gjennom arbeidskrafts innvandring. Norge kan være et attraktivt land for personer fra andre land å arbeide i. Her er gode arbeids-, pensjons- og lønnsforhold, en velfungerende offentlig sektor samt gode bo- og leveforhold.

Utfordringene med å tiltrekke seg utenlandsk arbeidskraft er flere. Det vil være en rekke IKT-sikkerhetsjobber som vil kreve sikkerhetsklarering og at kandidaten kan norsk. Samtidig viser en omfattende global undersøkelse, Global Information Security Workforce Study (2017), at det i år 2022 vil være en global mangel på IKT-sikkerhetspersonell på 1,8 mill. personer. Med andre ord så vil det være en stor global konkurranse om personell med den rette IKT-sikkerhetskompetansen. Dermed vil det i praksis være veldig vanskelig å importere arbeidskraft og lukke gapet på den måten.

Oversikten i kapittel 2 viser at det er få som tar en utdanning der hele utdanningsprogrammet er bygget opp rundt IKT-sikkerhet. Faktisk ser vi at av 505 kandidater uteksaminert i år 2016, er det bare 49 av disse som har gjennomført et studium der hele utdanningsprogrammet er bygget opp rundt IKT-sikkerhet. Dette svarer til beskjedne 10 prosent. Dette er trolig en utfordring fordi IKT-sikkerhet blir stadig mer kompleks, men omvendt er det ikke mulig å si hvor stor utfordringen er. Lysne-utvalget peker på at det er svært ønskelig at alle som gjennomfører en generell IKT-utdanning på høyere nivå, i forbindelse med utdanningen også tilegner seg grunnleggende kunnskaper om IKT-sikkerhet (Lysne-utvalget (2015)). Men hvorvidt det er nok til å imøtekomme fremtidens kompetansekrav, er usikkert.

Usikkert er det også i hvor høy grad fremtidig etterspørsel knytter seg til henholdsvis bredde- eller spisskompetanse. Vil det være et veldig stort behov for spesialister, eller blir det slik at alle relevante yrker må ha litt mer IKT-sikkerhetskompetanse? Svaret ligger nok midt imellom, men hvordan vektes det? Dette vil ha stor betydning for den fremtidige utdanningspolitikk og utdanningsdimensjonering.

[9] IKT-Norge har pekt på at det mangler mellom 6 300 og 8 600 personer med IKT-kompetanse i Norge, noe som gir en indikasjon.

5 Behovet for IKT-sikkerhetskompetanse – perspektiver fra norske aktører

Hovedkonklusjonen i fase I var at det i årene framover vil utdannes for få med kompetanse innen IKT-sikkerhet. Til tross for en betydelig økning i antall studenter og kandidater vil det være et økende gap mellom tilgang på og behov for personer med IKT-sikkerhetskompetanse. Våre estimater pekte på en underdekning på 4 100 personer med IKT-sikkerhetskompetanse. Dette er et tall som selvsagt må tas med forbehold. Men tallet må samtidig tas på alvor. Vi har i våre framskrivninger forsøkt å innarbeide økningen i antall studenter og uteksaminerte kandidater, men allikevel fant vi et betydelig udekket behov.

Det kan stilles en rekke oppfølgende spørsmål knyttet til resultatene fra fase I. Formålet med fase II er å få belyst flere av disse spørsmålene. Det fase I ikke svarer på, er hvordan tilbudssiden og etterspørselssiden ser ut i dag og hvordan de vil se ut i fremtiden, for eksempel når det gjelder spørsmål om tilbud på og behov for bredde- eller spisskompetanse innen IKT-sikkerhet, norske og internasjonale studenters overgang til norsk arbeidsmarked, muligheter for å tiltrekke seg en høyere andel kvinnelige studenter samt hvilke muligheter som ligger innen etter- og videreutdanning.

Det er viktig å få belyst disse spørsmålene, da det gir kunnskap om hvilke tiltak som kan eller må settes i verk, dersom kompetansebehovet skal dekkes.

I dette avsnittet presenteres informasjon og synspunkter vi har fått gjennom intervjuer av 18 informanter fra relevante forsknings- og utdanningsinstitusjoner, myndigheter, bransje- og interesseorganisasjoner og bedrifter. Oversikt over informantene fremkommer av metodebilag i vedlegget til rapporten. Vi har valgt å ikke fremheve enkeltsitater fra respondentene. Det er ikke enkeltutsagn som presenteres, men i stedet fremheves fellestrekkene i informantenes utsagn. I tilknytning til noen av temaene trekker vi inn annet relevant materiale for å supplere våre informanters utsagn. Til slutt i kapitlet drøfter vi kort om det er grunn til å stille seg kritisk til noe av det våre informanter forteller.

5.1 Norge blant verdens mest digitaliserte land, men har sikkerheten fulgt med?

Norge har vært langt fremme i å utvikle digitale løsninger for offentlig sektor, bredbåndsinfrastruktur, integrering av digitale løsninger, og landets innbyggere er i forkant når det gjelder bruk av IKT i hverdagen. Selv om Norge ikke er helt i tet, vi blir blant annet slått av land som Estland og Danmark, som skårer noe høyere på det som omtales som «gode» og «generelle» digitale ferdigheter (Digital Skills Indicator, 2016), er Norge like fullt blant de mest digitaliserte landene i EU og EØS

(Europakommisjonen, 2017). Et uttalt ønske om effektivisering av offentlige og private tjenester, som på sikt kan skape konkurransefortrinn i en internasjonal sammenheng, har på mange måter vært en sentral motivasjon for digitaliseringsprosessene vi har vært vitne til her til lands, og i land det er naturlig å sammenligne seg med.

Dette bildet har sammenheng med langsiktig arbeid og omfattende prosesser knyttet til digitalisering. Fremfor alt har arbeidet vært initiert av regjeringen og til en viss grad også til internasjonale trender og tiltak. For eksempel, hvis vi ser helt tilbake til 2003, lanserte OECD det som er omtalt som «e-Government Imperative», hvor et sentralt mål var å utforske mulighetene som fulgte med såkalte e-regjeringsinitiativer. Slike tiltak skulle: "bolster government effectiveness in important ways like facilitating cross-agency cooperation on complex problems, fostering a customer focus for services, and building relationships with private sector partners" (OECD, 2003). Videre pekte OECD-rapporten på at forsinkelse i implementeringen av slike e-regjeringsreformer i verste fall ville kunne bremse økonomisk utvikling (ibid.). Disse signalene kan ha påvirket regjeringer med tanke på hvordan fortsette videre utvikling av teknologi- og digitaliseringsprosesser. Få år etter denne innledende rapporten, publiserte OECD landrapporter om utvikling og utfordringer på e-forvaltning for henholdsvis Norge (2005) og Danmark (2006). For Norges del ble en oppfølgingsstudie publisert høsten 2017 (OECD, 2017).

En utfordring som flere av våre informanter adresserer, handler om bekymringer for at digitaliseringsprosessen faktisk har gått for raskt og at man ikke i tilstrekkelig grad har klart å identifisere og ivareta utfordringer knyttet til sikkerhet når tidligere analoge tjenester og systemer har blitt digitalisert. Innledningsvis viste vi til flere eksempler der IKT-sikkerheten på ulike måter hadde blitt utfordret eller ikke tilstrekkelig ivaretatt.

Satsing på utdanning som dekker ulike sider ved digitalisering og herunder også utdanning knyttet til kompetanse i IKT-sikkerhet, er slik eksempler på at Norge nå faktisk «henger etter» og møter utfordringer for å dekke samfunnets behov for slike kompetanser.

Et annet område mange av informantene trekker frem som kritisk, og som omfatter dimensjoner av IKT-sikkerhet, er det som ofte kalles 'Tingenes internett', eller Internet of Things (IoT). Dette er et samlebegrep for nettverk av identifiserbare gjenstander som er utstyrt med elektronikk, programvare, sensorer, aktuatorer og nettverk som muliggjør at gjenstandene kan koble seg til hverandre og utveksle data (Teknologiradet.no), og slike nettverk gjelder på alle nivåer i samfunnet; fra makro-, meso- til mikronivå. Våre informanter peker på betydningen av å tenke IKT-sikkerhet som en integrert del av produktutvikling, enten det er helsesystemer, smartklokker eller integrerte kameraer i leketøy. Ikke bare er dette viktig for den aktuelle målgruppen designet er laget for, like viktig er det at produkter over tid kan endres og bli brukt i nye sammenhenger. Dersom sikkerheten ikke er tilstrekkelig ivaretatt i designet, kan nye sårbarhetssituasjoner oppstå.

Denne typen bevissthet og kunnskap fremheves som avgjørende av våre informanter på tvers av sektorer og bransjer. Her viser de med andre ord til at nettopp på grunn av utbredelsen av IoT er samfunnet avhengig av IKT-infrastruktur og løsninger som krever at informasjonssikkerhet er en kritisk egenskap ved all teknologi vi omgir oss med. Dette betyr at IKT-sikkerhet både inngår som en del av det vi kan kalle generelle moderne ferdigheter i vår tid – ofte omtales dette også som en del av 21st Century Skills[10], og disse gjelder slik for alle borgere. I tillegg til at spesialisert IKT-sikkerhetskompetanse er helt avgjørende for et moderne samfunn, noe som understrekes i vårt innledende kapittel 1.

[10] For mer informasjon om 21st Century skills, se https://en.wikipedia.org/wiki/21st_century_skills .

5.2 Tilbud og etterspørsel, status per i dag og i årene som kommer

Vår konklusjon basert på økonomiske modeller og statistikk er at det er en betydelig underdekning av personer med adekvat IKT-sikkerhetskompetanse i norsk arbeidsliv. Hvorvidt det rent faktisk oppleves slik per i dag, har vi undersøkt ved å intervjue myndigheter, bedrifter, arbeidsgiver- og arbeidstakerorganisasjoner samt forsknings- og utdanningsinstitusjoner.

5.2.1 Dagens status for tilbud og etterspørsel

Den overordnede konklusjon basert på intervjuene er at det allerede per i dag er en betydelig underdekning av personer med IKT-sikkerhetskompetanse. Informantene peker dermed på samme utfordring omkring gap mellom tilbud og etterspørsel for IKT-sikkerhetskompetanse, som det som fremkom via de kvantitative analysene.

Blant argumentene som informantene peker på, er at studenter blir tilbudt jobb og har signert kontrakt 12–18 måneder før de er ferdig utdannet. Dette er selvsagt positivt for studenten, som ikke behøver å bekymre seg for jobbsituasjonen etter endt utdanning. Den store etterspørselen gjør at det er vanskelig for arbeidsgivere å rekruttere nyutdannede. Det må gjøres en ekstra innsats dersom man vil tiltrekke seg de riktige kandidatene, hva enten det er å tilby en lønn som er vesentlig høyere enn det andre akademikere tilbys, eller det er å gjøre en særlig rekrutteringsinnsats, for eksempel å fly til en annen del av landet og spise middag med en potensiell kandidat for på den måten å kapre talentet.

Det er ikke alltid avgjørende hvilke spisskompetanser kandidaten har, mener flere av informantene. Det handler i nokså høy grad om at kandidaten har en basisforståelse for et område og en attityde og et engasjement for å jobbe med IKT-sikkerhet. Da kan intern utvikling og opplæring kompensere for at kandidaten eventuelt mangler den rette spisskompetansen. Dessuten går utviklingen innen IKT-sikkerhet så fort at det uansett er et løpende behov for å tilegne seg ny viten og kompetanse. Dermed er det ikke avgjørende hvilke spisskompetanser den nyansatte har. For kandidatene er det lite incentiv til å utfordre seg selv faglig, eller gjøre en innsats for å lære sig komplisert stoff.

Flere av våre informanter peker på at det i de senere år har vært en betydelig økning i fokus på IKT-sikkerhet. Vi ser at stadig flere ressurser allokeres til feltet. Bemanningen øker betydelig der sysselsettingen dobles eller flerdobles. De som har bygget opp en forretningsmodell rundt IKT-sikkerhet og har sørget for å få kompetanse til å understøtte forretningsfokuset, har gode dager.

Det har vært en betydelig økning i etterspørselen, og her har tilbudssiden ikke har klart å følge med. Til tross for at det lenge har vært et fokus på behovet, har man ikke lykkes med å mobilisere tilstrekkelig med ressurser og kompetanse. Våre informanter peker på at en del av forklaringen kan være en manglende modenhet når det gjelder å se behovet. Og at det kan være en av årsakene til at det er en manko i dag.

5.2.2 Fremtidens behov

Dagens betydelige underdekning av personer med adekvat IKT-sikkerhetskompetanse vil ifølge våre informanter øke i fremtiden. Flere av informantene peker på at det de seneste år har vært en markant utvikling innenfor IT og internett i alle slags produkter; det gjelder leketøy, dukker, kjøleskap, biler og el-måleren din, det såkalte «Internet of things». Dermed blir samfunnet avhengig av IKT-strukturer og IKT-løsninger, og IKT-sikkerhet blir en kritisk egenskap ved de tingene vi omgir oss med. Dette stiller krav til bedrifter i de næringene som tilbyr leketøy, kjøleskap, bil eller el-måler. Alle må tenke IKT-sikkerhet og ha personer ansatt som kan sikre at produktutviklingen tar inn over seg IKT-sikkerhet. Dette vil øke fremtidens behov for personer med IKT-sikkerhetskompetanse, påpeker våre informanter.

Flere av våre informanter har pekt på behovet for å styrke kompetansen sin i forbindelse med ny EU-forordning og den nye personvernloven som kommer i mai 2018. Personvernloven gir personer først og fremst flere rettigheter med hensyn til å skaffe seg kontroll over hvilke data andre har registrert om henne/ham[11]. Når vi etterlater oss digitale spor på Facebook, bruker Google, registrerer løpeturen med Strava og våre innkjøp med Æ (Rema1000 sin app), gir de nye reglene oss rettigheter til sporene som vi ikke tidligere hadde. De nye reglene stiller krav til bedriftene. De må ha systemer som kan håndtere rettighetene til enkeltpersoner på en hensiktsmessig måte.

Den nye personvernforordningen har særlig fokus på IKT-sikkerhet og stiller nye krav, peker flere av våre informanter på. De peker på at tidligere kunne bedrifter ha en sikkerhetspolicy og få hjelp til å utarbeide en slik policy. Med den nye forordningen stilles det andre krav. Nå må virksomheter, både offentlig og private, ha verktøy som sikrer at det ikke er huller i sikkerheten. Selskapet Trend Micro fant 433 000 søkbare enheter tilkoblet internett i Oslo. Og er de søkbare, kan de i teorien også bli utsatt for angrep, noe som fremheves var grunnlaget for Mirai-angrepet i 2016 og Wannacry i 2017. De enheter som nevnes i rapporten til Trend Micro, er overvåkningsutstyr, babymonitorer, medisinsk utstyr, husholdningsapparater og databaser [12]. Konsekvensene av brudd på IKT-sikkerheten, som disse 433 000 enhetene potensielt er eksempler på, er flere. Det er risikoen for angrep, som man er vesentlig mer eksponert for, når man er søkbar. Og den nye personvernforordningen stiller krav om at eventuelle brudd på sikkerheten rapporteres til Datatilsynet innen 72 timer og at bruddet/hullet blir lukket med en gang. Dersom organisasjonen ikke klarer å imøtekomme et slikt krav, venter det bøter på opptil 4 prosent av omsetningen. Dette gjelder også for offentlige virksomheter.

I tillegg til å måtte leve opp til den nye personvernforordringen blir forordningen et potensielt mål for utpressing. De høye bøtene som følger en eventuell manglende sikkerhet, setter virksomheter, både offentlige og private, i en vanskelig situasjon, der trusler om avsløring av sikkerhetshull fra kriminelle kan gjøres til gjenstand for utpressing[13]. De nye krav og den økte fokus på IKT-sikkerhet er igjen med på å øke forventningene til fremtidens etterspørsel etter IKT-sikkerhetskompetanser.

Samlet peker våre respondenter på at i årene som kommer, vil etterspørselen fortsette å øke. Driverne er, ut over personvernforordringen:

- Knyttet til stadig større utbredelse av IKT, tingenes internett, man bruker IT stadig mer avansert, og da blir IKT-sikkerhet mer aktuelt.

- Det stilles større krav til leverandører omkring sikkerhet i IKT-løsninger, noe som langt fra alle leverandører per i dag kan leve opp til, og de må derfor øke kompetansen sin innen IKT-sikkerhet.

- IKT-sikkerhet må fremover tenkes inn som en integrert del av designet og utviklingen av nye produkter og tjenester. Det hjelper ikke å legge IKT-sikkerhet til i etterkant. Dette betyr at IKT-sikkerhet kommer til å inngå som en sentral del av innovasjonsaktivitetene i både offentlig og privat sektor.

- Datakriminalitet ser globalt sett ut til å ha blitt mer organisert. Det er til stadighet mer profesjonelle angrep. Hackeren ble tidligere sett på som en nysgjerrig fyr – nå har han mulighet til å drive med sabotasje og organiserte businessmodeller med hacking. Et eksempel på dette er at datakriminalitet nå er den største økonomiske kriminalitetsformen i Storbritannia.

[11] Se https://www.digi.no/artikler/kronikk-gdpr-styrker-rettighetene-til-mannen-i-gata-men-hva-er-egentlig-gdpr/387839
[12] Se Dagens Næringsliv 4. desember 2017 og https://documents.trendmicro.com/assets/wp/wp-western-europe-cities-exposed.pdf
[13] Se ComputerWorld artikkel fra 12. desember 2017: «Snart starter GDPR-svindelen».

- Det er allerede per i dag et betydelig etterslep innen IKT-sikkerhetskompetanse. Bare å lukke det nåværende gapet vil kreve en betydelig økning av antall personer med IKT-sikkerhetskompetanse i løpet av de neste 3 til 5 årene.

Synspunktene fra våre informanter understøtter framskrivningen i kapittel 3, som pekte på en markant økning i etterspørselen og dermed et økt gap på tilbudssiden for IKT-sikkerhetskompetanse. De nevnte driverne underbygger at det er behov for å øke tilbudssiden enda mer enn det som allerede er tilfellet.

5.3 Hvilke muligheter finnes for å øke og supplere tilbudssiden

Ifølge våre informanter haster det med å få økt tilbudssiden. Det finnes en stor og udekket etterspørsel i dag, og de fleste respondentene peker på at etterspørselen vil øke i årene fremover. I våre intervjuer er det blitt pekt på innsatser som må til for å øke tilbudssiden. Det gjelder både tiltak som kan ha en umiddelbar effekt, men også tiltak som har en mer langsiktig effekt på økningen av tilbudssiden.

5.3.1 Flere generalister og flere spesialister, det trengs mer av alt

Tallene i tabell 1 og 2 viser en betydelig økning i antall studenter og uteksaminerte kandidater. Dessuten viser de at rundt 10 prosent av kandidatene og studentene i en årgang har et utdanningsløp med flere fag knyttet til IKT-sikkerhet. Disse personene velger vi å kalle spesialister innen IKT-sikkerhet, mens de øvrige 90 prosent i høyere grad vil være IKT-generalister, i mangel av et bedre uttrykk.

Vi har i forbindelse med intervjuer av nøkkelpersoner vært opptatt av om denne fordelingen var problematisk. Når det i forveien er en manko på personer med IKT-sikkerhetskompetanse, er da faktumet at «bare» 10 prosent av de nyutdannede er spesialister et problem? Eller er markedets behov av en slik natur at man først og fremst trenger folk, og dernest kan disse personene oppkvalifiseres slik at de matcher kompetansebehov? Fordelingen mellom «spesialister» og «generalister» kan slik være av mindre betydning. Svarene vi har fått gir ikke noe entydig svar, men gir dog en viss nyansering.

Flere generalister
Det er samlet sett et ønske om å heve antallet kandidater med IKT-sikkerhetskompetanse. Her er det mange av våre informanter som påpeker at IKT-sikkerhet må inn som et «ikke-valgfritt» (obligatorisk) fag på alle IKT-utdanninger. Faktisk peker flere på at faget IKT-sikkerhet må inn på alle teknologi-utdanninger, noe som også Kunnskapsdepartementet er opptatt av og som kan bli implementert allerede i forbindelse med justering av forskrift om rammeplan for ingeniørutdanning. Dermed er det et krav som Kunnskapsdepartementet stiller til utdanningsinstitusjonene. Et slikt krav harmonerer dårlig med utdanningsinstitusjonenes krav om autonomi, men som flere informanter fremhever, er mangelen på IKT-sikkerhetskompetanse en grunnleggende nasjonal og samfunnskritisk utfordring, som må møtes.

Flere spesialister
Det vil også være behov for å heve antallet studenter på de spesialiserte utdanningsløpene. Det er ikke nødvendigvis de personene næringslivet og offentlig sektor har størst behov for her og nå, påpeker informantene våre. Men behovet for dyktige kandidater som kan gå i gang med et doktorgradsstudium, senere en post doc. og til slutt ende opp som undervisere og forskere er stor. Dette er opplagt av en mindre dimensjon enn når vi taler om behovet for IKT-sikkerhetskompetanse generelt, men utfordringen er ikke mindre kritisk.

Våre informanter, særlig innen UH-sektoren, peker på at det er stor mangel på dyktige kandidater som velger å ta en doktorgrad og et videre karriereløp innen forskning og utdanning. Dette, påpeker de, er kritisk for neste generasjon av undervisere innen høyere utdanning. Og det er kritisk for de delene av samfunnet der de mest kompetente innen IKT-sikkerhet skal jobbe. Et eksempel som ble trukket frem

nå nylig, er behovet for kryptologer[14]. Status for kryptologer er at ingen personer er i gang med en doktorgrad. Det betyr også at rekrutteringsgrunnlaget for fremtidige undervisere er sterkt utfordret, særlig siden de nåværende underviserne er få og oppe i årene.

Samtidig peker flere av våre informanter fra UH-sektoren på at det er vanskelig å motivere dyktige studenter fra Norge eller de nordiske land til å gå i gang med doktorgradsstudier. En åpenbar forklaring er dagens store etterspørsel etter personer med IKT-sikkerhetskompetanse. Når bortimot alle studerende i et kull blir tilbudt jobb 12–18 måneder før de er ferdige (for eksempel med en masterutdanning), er de fleste sannsynligvis lite motivert for å heve seg faglig og velge et doktorgradsstudium. Da handler det nok i større grad om å bli ferdig, så hurtig og enkelt som mulig og så komme seg ut i arbeidslivet med de goder som det fører med seg, pekes det på fra våre informanter.

På tvers av informantene var det en klar anbefaling å øke utdanningskapasiteten. Som nevnt i det ovenstående var det et vesentlig poeng å få flere kandidater gjennom utdanningen, slik at de kommer ut på arbeidsmarkedet med basiskompetanse. En utfordring med å øke utdanningskapasiteten er å få inn gode studenter, som har den rette interessen for området og en viss forståelse for IKT. Derfor har flere av våre respondenter pekt på at IKT og IKT-sikkerhet bør inngå som en del av undervisningen på videregående skole eller i ungdomsskolen. Et slikt fag vil gi de unge kunnskap om håndtering av hvilke informasjoner de deler på nett og hvordan de beskytter seg selv på nett. Når vi vet at digital dømmekraft allerede er en sentral del av digital kompetanse, kan man i så måte vurdere å supplere med flere sider av IKT-sikkerhet enn det dagens læreplaner omfatter.

5.3.2 Øk utdanningskapasiteten og bruk eksterne undervisere

Vi ser at utdanningskapasiteten øker. Samtidig poengteres det fra den sittende regjering at det allokeres stadig flere ressurser til utdanning. Det pekes på at det i 2018 er avsatt penger til opprettelse av 500 nye studieplasser innenfor IKT og at Kunnskapsdepartementet ved tildeling vil be institusjonene om å prioritere tilbud som er viktige for IKT-sikkerhet og kryptologi[15].

Penger til nye studieplasser må rent faktisk omsettes til konkrete studieplasser, påpeker flere av våre informanter. Gjennom forslag om endring av forskrift om rammeplan for ingeniørutdanning, kan det tyde på at det vil bli et krav fra Kunnskapsdepartementet[16]. Men hvor hardt dette ønsket fra Kunnskapsdepartementet blir betonet er vanskelig å si. Og dermed kan man håpe at pengene ikke havner andre steder enn det som var intensjonen.

Flere studieplasser og flere ressurser krever flere undervisere. Dette er en utfordring som kan være vanskelig å løse for utdanningsinstitusjonene, påpeker flere informanter fra UH-sektoren. Det er allerede betydelige undervisningsforpliktelser for eksisterende undervisere. Og med mangel på doktorgradsstudenter og personer i post doc.-stillinger er det ikke opplagt hvor personer som skal undervise disse 500 nye studentene, skal komme fra.

En mulig løsning er å hente inn eksterne undervisere. Dette er noe flere av våre respondenter har hevdet. Det vil kunne imøtekomme den stigende etterspørselen etter undervisningskompetanse. Og samtidig er det behov for å få det praksisnære og anvendelsesorienterte inn i undervisningen. IKT-sikkerhet bygger selvsagt på en god teoretisk forståelse, men utviklingen skjer så fort at det er et opplagt behov for å dra inn det anvendelsesorienterte og praksisnære i utdanningene.

En annen utfordring er kvaliteten på søkerne. Som det nevnes av en respondent, har antall studieplasser innenfor informasjonssikkerhet doblet seg. Og det er mange søkere, men kvaliteten

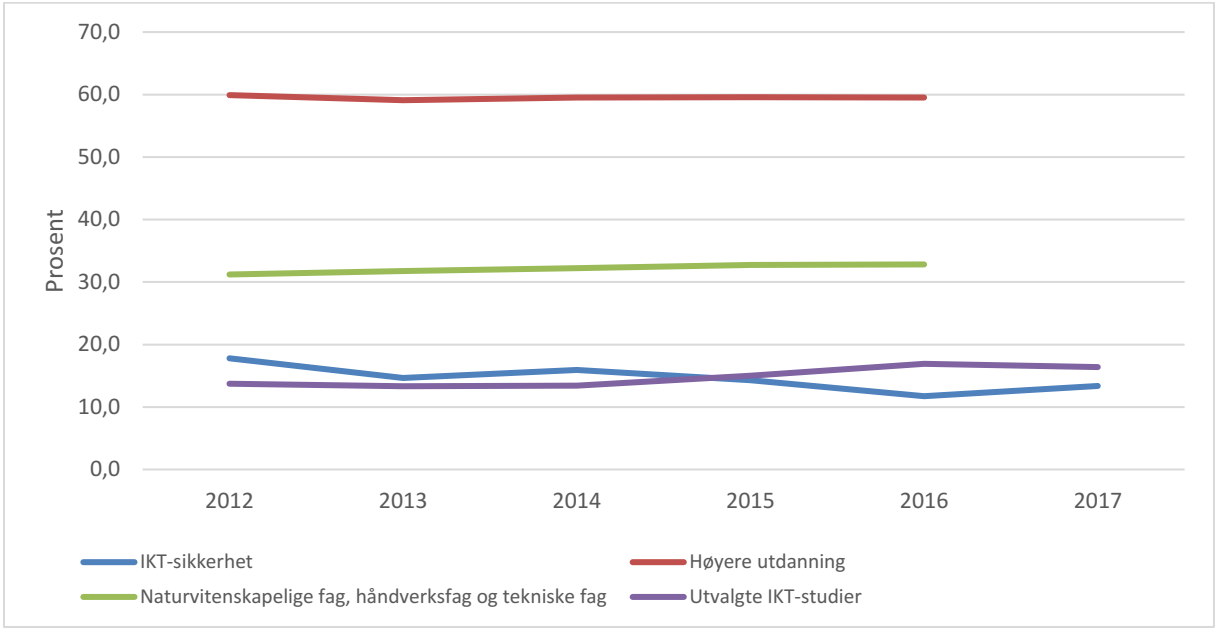
[14] Se Dagens Næringsliv 02-12-17, DN Magasinet
[15] Se statsministerens skriftlige svar til Jonas Gahr Støre 14 desember 2017. Skriftlig spørsmål fra Jonas Gahr Støre (A) til statsministeren, dokument nummer 15:436(2017-2018).
[16] Se Høring - justering av forskrift om rammeplan for ingeniørutdanning, Kunnskapsdepartement 04.12.2017.

kunne vært bedre. Dette er noe utdanningene strever med. En mulig løsning er å få IKT og IKT-sikkerhet inn i timeplanen både i grunnskolen og i videregående skole.

Samtidig bør også kvinneandelen økes. Tradisjonelt er kvinnene eller jentene kraftig underrepresentert på IKT-utdanninger. Og dette er ikke annerledes innen IKT-sikkerhet. Våre respondenter mener dog at situasjonen bedrer seg og at de og andre har stort fokus på å rekruttere flere. Arrangementet «security divas» blir nevnt i denne sammenhengen; gjennom de seneste 7–8 årene har det samlet ca. 140 kvinner fra hele verden.

Våre informanters synspunkt understøttes ikke umiddelbart av utdanningsstatistikk fra DBH. Statistikken viser at antall kvinnelige studenter innen IKT-sikkerhet faktisk har vist en synkende tendens de siste fem år. I 2016 var 13,4 prosent av studentene innen IKT-sikkerhet kvinner. Dette er ikke enestående for Norge, globalt fremheves det at kun 11 prosent av de som jobber med cybersikkerhet, er kvinner i verden (Frost & Sullivan, 2017).

Figur 3: Prosentandel kvinner av studenter i utdanninger i IKT-sikkerhet på bachelorgradsnivå eller høyere, sammenlignet med andre studenter i høyere utdanning.



Kilde; DBH og SSB, statistikkbanken.

Nivået for IKT-sikkerhetsfag er omtrent som for andre IKT-fag, men mens kvinneandelen har økt litt for den sistnevnte gruppen i den perioden vi ser på, har den sunket litt for IKT-sikkerhetsfag. Nielsen (2002) finner at kvinneandelen blant kandidater som avla embetseksamen eller hovedfag i IKT-fag generelt i perioden 1981–1996, var 19 prosent. Det synes altså ikke å være noen tegn til at andelen øker. Dette føyer seg inn i et generelt mønster; selv om andelen kvinner som tar høyere utdanning har økt kraftig, er det små endringer i de faglige preferansene.

Det viser seg med andre ord at den innsatsen som er gjort for å øke andelen av kvinner innen IKT-sikkerhet, så langt tilsynelatende ikke har hatt noen stor effekt. Det krever selvsagt en mer omfattende studie å undersøke om det rent faktisk er tilfellet og hva det eventuelt kan skyldes. Tallene indikerer at dette er et tema som nok er kommet høyere på dagsordenen, men som fortsatt har behov for et betydelig fokus.

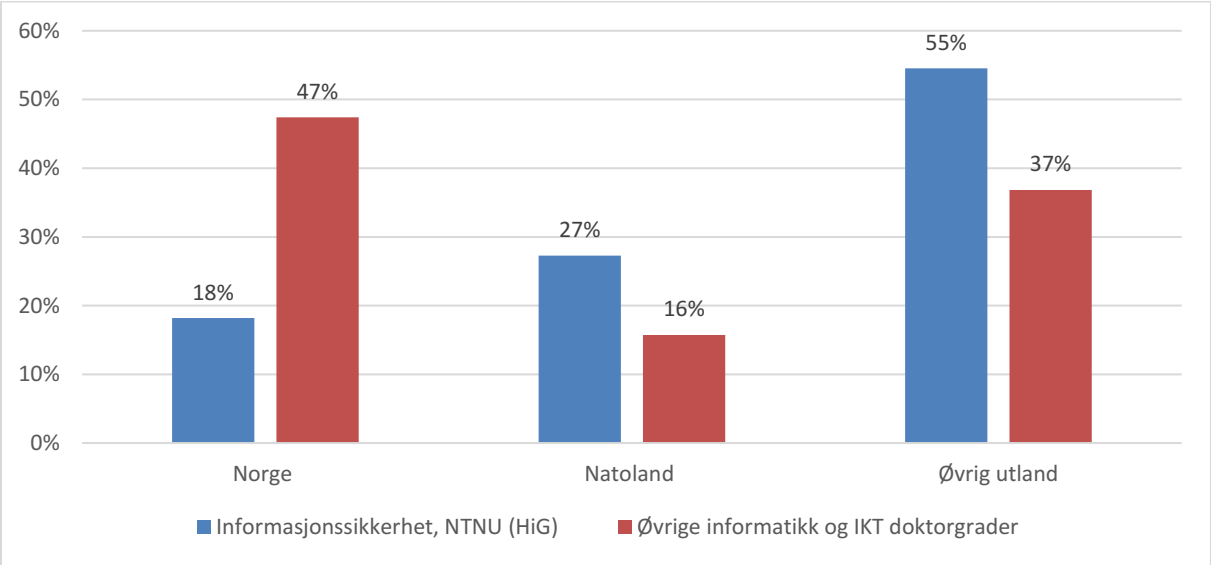
5.3.3 Styrk grunnlaget for forskningsbasert utdanning

Flere av våre informanter pekte på utfordringen rundt den begrensede muligheten til å øke undervisningskapasiteten. Det er en utfordring å klare å utdanne flere spesialister og da særlig norske eller nordiske spesialister. Med den betydelige etterspørselen er det stor konkurranse om de dyktigste

kandidatene, som kan være relevante å ta opp på doktorgradsstudier, og som senere kan tre inn i rekken av undervisere ved høyere utdanningsinstitusjoner.

Via et spesialuttrekk fra NIFUs doktorgradsregister har vi sammenfattet fordelingen av avlagte doktorgrader de seneste 10 årene, det vil si 2007–2016. Tallene er fordelt mellom de som har tatt doktorgrad i informasjonssikkerhet på NTNU (HiG), og de som har tatt doktorgrad i øvrige informatikk- og IKT-studier, der IKT-sikkerhet kan ha vært tema i studiet, men i de langt fleste tilfellene ikke er det. De siste 10 årene er 45 prosent av de som har tatt doktorgraden sin innen IKT-sikkerhet, fra Norge eller annet natoland. 55 prosent er altså fra ikke-natoland. Det bør i tillegg poengteres at kun 11 personer har tatt doktorgrad innen IKT-sikkerhet de siste 10 årene.

Figur 4: Avlagte doktorgrader i perioden 2007–2016 fordelt på Norge, Natoland og øvrig utland.



Kilde: Doktorgradsregisteret, NIFU, spesialkjøring desember 2017.
Note: N=11 for Informasjonssikkerhet, N=559 for øvrig informatikk og IKT. Øvrig informatikk og IKT dekker utdanningsinstitusjonene Universitetet i Bergen, Universitetet i Oslo, Universitetet i Stavanger, Universitetet i Agder samt Norges teknisk-naturvitenskapelige universitet med Høgskolen i Gjøvik.

En annen utfordring som trekkes frem av våre informanter, er de få og små fagmiljøene som finnes rundt om på utdanningsinstitusjonene. De lærestedene som har et fagmiljø av en viss størrelse, vil enklere kunne tiltrekke seg doktorgradsstudenter enn miljøer hvor dette ikke er tilfellet, hevder våre respondenter. Det samme gjør seg gjeldende for bedrifter og offentlige myndigheter, hvor et fungerende fagmiljø i tillegg til en god lønn er avgjørende tiltrekningsfaktorer. Dermed blir også små miljøer ofre for en selvforsterkende effekt og taper terreng til de større miljøene.

I Meld. St. 10 «Risiko i et trygt samfunn» (Justis- og beredskapsdepartementet, Regjeringen Solberg, 2016) poengteres også viktigheten av forskning og den forskningsbaserte utdanning:

> *Flere forskere og gode forskningsmiljøer er viktig av flere grunner. Forskning bidrar til innovasjon, sikkerhet i nye produkter og ny kunnskap. Gode forskningsmiljøer bidrar til forskningsbasert utdanning og økt veiledningskapasitet. Bedre kvalitet i utdanning vil kvalifisere flere norske til ph.d. Det er også viktig med et visst volum, både på antall forskere og forskningsmidler, for at det skal bli høy kvalitet på forskningsmiljøene.*

Våre respondenter peker dog på at en økning gjennom de tradisjonelle kanalene ikke er tilstrekkelig. Det er flott at eksempelvis IKTPLUSS har blitt etablert. Men et behov for nytenkning fremheves. Som det også fremgår av Meld. St. 10 (Justis- og beredskapsdepartementet, Regjeringen Solberg, 2016), er samarbeidsinitiativer viktige, noe som er en betydelig styrke for Center for Cyber and Information Security (CCIS). Respondentene peker på at initiativer og grupper som klarer å skape en arena for

samarbeid mellom forskere, myndigheter, myndigheter med sikkerhetsansvar og privat næringsliv med førstehåndskunnskap til utfordringer, vil være sentrale. Som tidligere nevnt handler det om å få dratt inn det anvendelsesorienterte og praksisnære i utdanningene, for utviklingen går fort. Flere av våre informanter peker på at det godt kan avsettes flere midler til forskning innen IKT-sikkerhet, men da må en betydelig del av disse gå til å bygge opp samarbeidsinitiativ og arenaer eller grupper, hvor kravet om deltakelse ikke bygger på antall siteringer eller publiseringer, men i større grad en på en vurdering av førstehåndskjennskap til hva som trenges for å møte de samfunnskritiske utfordringene knyttet til IKT-sikkerhet.

5.3.4 Sats på etter- og videreutdanning

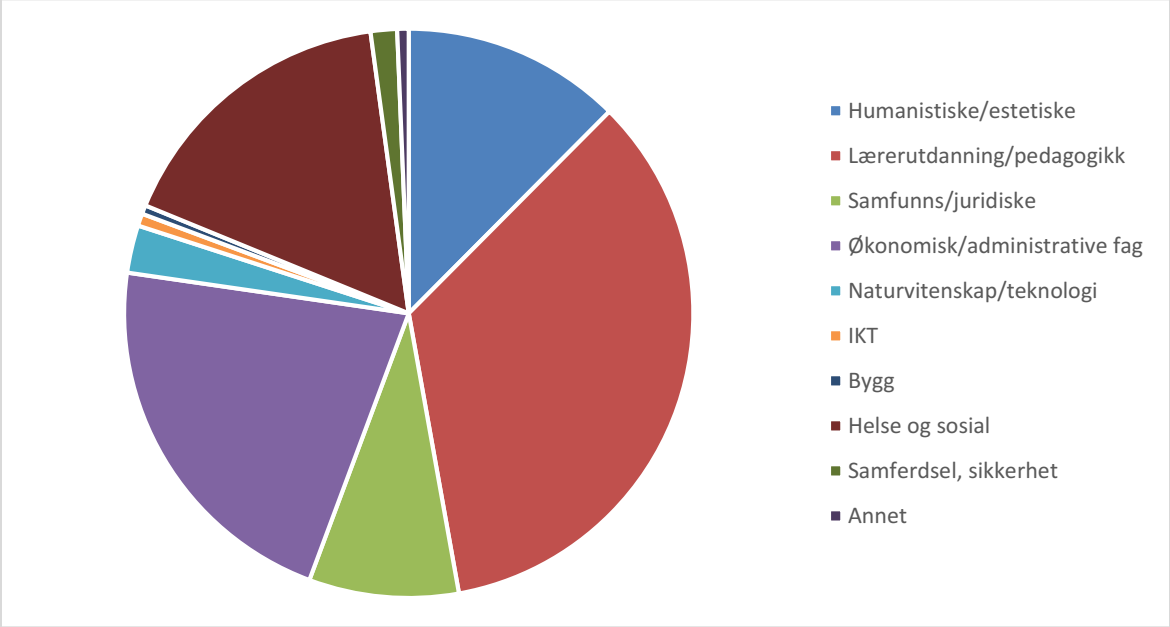
Gjennom intervjuene i studien vår ble det pekt på at det er et uttalt behov for IKT-sikkerhetskompetanse på de fleste områder i samfunnet. Samtidig fremhevet mange også behovet for sektorspesifikk – eller områdespesifikk – kompetanse koblet sammen med IKT-sikkerhetskompetanse. Våre informanter peker for eksempel på at helsepersonell trenger kunnskap om hvordan håndtere sensitive pasientdata, i skolen trenger lærere og skoleledere tilsvarende kjennskap til elevdata og tilsvarende for andre profesjoner og områder av samfunnet. Mange informanter var også tydelige på at slike hybridkompetanser må tilegnes som en del av livslang læring og i form av etter- og videreutdanningsløp. Slik kan ansatte i arbeid oppnå spisskompetanse innenfor IKT-sikkerhet og selv tilpasse den til egen bransje eller sektor.

Ser vi på hvordan etter- og videreutdanningslandskapet ser ut innenfor universitets- og høgskolesektoren, finnes slike tilbud tilsynelatende i ganske begrenset omfang. Innenfor universitets- og høgskolesektoren kan skillet mellom eksplisitte versus implisitte videreutdanningstilbud være vanskelig å identifisere. For eksempel kan enkeltstående emner som inngår i bachelor- eller masterprogram og som tilbys av universitet og høgskoler, i enkelte sammenhenger også tilbys som videreutdanningstilbud for kvalifiserte søkere. I tillegg kan hele utdanningsprogram tilsynelatende fungere som videreutdanningstilbud for noen idet de begynner på nye utdanningsløp etter å ha vært i arbeid.

Da NIFU kartla etter- og videreutdanningstilbydere i Norge i 2015 fant vi et svært begrenset antall videreutdanningstilbud som omfattet IKT generelt (Tømte, et al., 2015). Vi kan videre anta at det dermed var enda færre videreutdanningstilbud som omfattet IKT-sikkerhet. Figuren nedenfor er hentet fra nevnte rapport og viser fordelingen av videreutdanningstilbud fordelt på utdanningsområder. Kartleggingen brukte fagkodene i Norsk standard for utdanningsgruppering.[17] Figur 5 gir en oversikt over antall tilbud på de forskjellige fagområdene.

[17] https://www.ssb.no/utdanning/norsk-standard-for-utdanningsgruppering

Figur 5: Fordeling av tilbud innen etter- og videreutdanning mellom fagområder



Kilde: Tømte et al (2015)

Figuren viser at nærmere 35 prosent av tilbudene er innen lærerutdanning/pedagogikk og 22 prosent innen økonomi og administrasjon. Innen økonomi og administrasjon finner vi videreutdanning i prosjektledelse, som også gis av mer teknologiorienterte fagmiljøer, og dette kan være en årsak til at det er relativt få videreutdanninger i disse fagene. Med tanke på den potensielt store etterspørselen kan det virke overraskende at bare 1 prosent av EVU-kursene er innen IKT.

Dette er også noe våre respondenter peker på. De peker på at det ikke er mange etter- og videreutdanningstilbud, men det finnes noen få kurs man kan ta. Samtidig peker de på at de opplever at det er en betydelig etterspørsel etter tilbud innen etter- og videreutdanning, noe som blant annet skyldes at den tekniske utviklingen skjer så fort at det studentene har lært på studiene fort blir utdatert. Derfor er åpenbart etter- og videreutdanning en mulig løsning.

Derfor kan det virke litt overraskende at det ikke tilbys et større mangfold av kurs innen IKT-sikkerhet. Våre informanter mener at en mulig forklaring er at det er et spørsmål om ressurser på utdanningsinstitusjonene, der underviserne har undervisningsbelastning fra før. Samtidig peker flere av våre informanter på at det også burde være mulig å få inn praktikere til å undervise. Men dette vanskeliggjøres av organiseringen i UH-sektoren, der man er tilbakeholden med bruk av eksterne undervisere til undervisning i fag som gir studiepoeng, pekes det på av våre informanter.

Til slutt peker flere informanter på utfordringer i finansieringsstrukturen og hvem som betaler. Om etter- og videreutdanningen ikke er en del av gradsstudier, blir det en annen type finansiering, og dermed en potensiell barriere. Det er ikke mulig for oss i dette prosjektet å gå nærmere inn i spørsmål om finansieringsstrukturen og insitamentsstrukturen for å tilby etter- og videreutdanning innen IKT-sikkerhet, men det ser ut til at det her kan være en barriere som bør håndteres.

Universitet og høgskoler som tilbyr etter- og videreutdanning, finansierer sine tilbud på ulike måter; gjennom studieavgift, ekstern finansiering som Kompetanse for Kvalitet, intern finansiering og gjennom at lærestedene får betalt per produserte studiepoeng. Kartleggingen av EVU-tilbud i UH-sektoren fra 2015 viste en stor variasjon i studieavgifter for videreutdanningstilbudene. For 443 tilbud var det ikke oppgitt pris, og flesteparten av disse var innenfor lærerutdanning/pedagogikk og helse/sosial.[18] For 271 av tilbudene ble det innkrevd studieavgift, mens det for de resterende 836

[18] For lærerutdanning/pedagogikk henger dette trolig sammen med myndighetenes satsing Kompetanse for kvalitet.

programmene – altså litt over halvparten – var deltakeravgift.[19] Avgiften varierte fra litt over 1000 kroner til 370 000 kroner for en «Master of Business and Administration i strategisk ledelse» som går over to år. Mest vanlig er det med deltakeravgift på programmer innenfor ledelse, økonomi og administrasjon samt noen helsefag som sykepleie. Konkurransen fra andre læresteder er med på å bestemme prisen på deltakeravgiften, enten ved at prisen settes ned dersom mange tilbyr lignende tilbud, eller går opp dersom tilbudet er unikt i markedet (Tømte, et al., 2015).

Det er imidlertid ikke noen fullgod forklaring på det manglende tilbudet. Vi vil derfor foreslå at dette undersøkes nærmere og at etter- og videreutdanning får en sentral plass i den kommende nasjonale kompetansestrategien innen IKT-sikkerhet. Det vil også være helt naturlig i forlengelsen av fokus på etter- og videreutdanning fra Meld. St. 38 IKT-sikkerhet (Justis- og beredskapsdepartementet, Regjeringen Solberg, 2017), hvor det heter at: «Det er viktig at det gis tilbud om etter- og videreutdanning til personer som har behov for IKT-sikkerhetskompetanse på arbeidsplassen. (…) både studiepoenggivende etter- og videreutdanning, sertifiseringskurs og andre målrettede IKT-sikkerhetskurs er nødvendige.»

5.3.5 Internasjonal rekruttering

Gjennom våre intervjuer har vi drøftet muligheten for å rekruttere internasjonalt. Det viser seg å være en løsning som mange av våre informanter benytter seg av. I forbindelse med internasjonal rekruttering har det vært naturlig for våre informanter å drøfte spørsmål om sikkerhetsklarering. Internasjonal rekruttering fra andre nordiske land er klart å foretrekke. Om det ikke er fra nordiske land, er det greit å sikkerhetsklarere personer fra andre Nato-land.

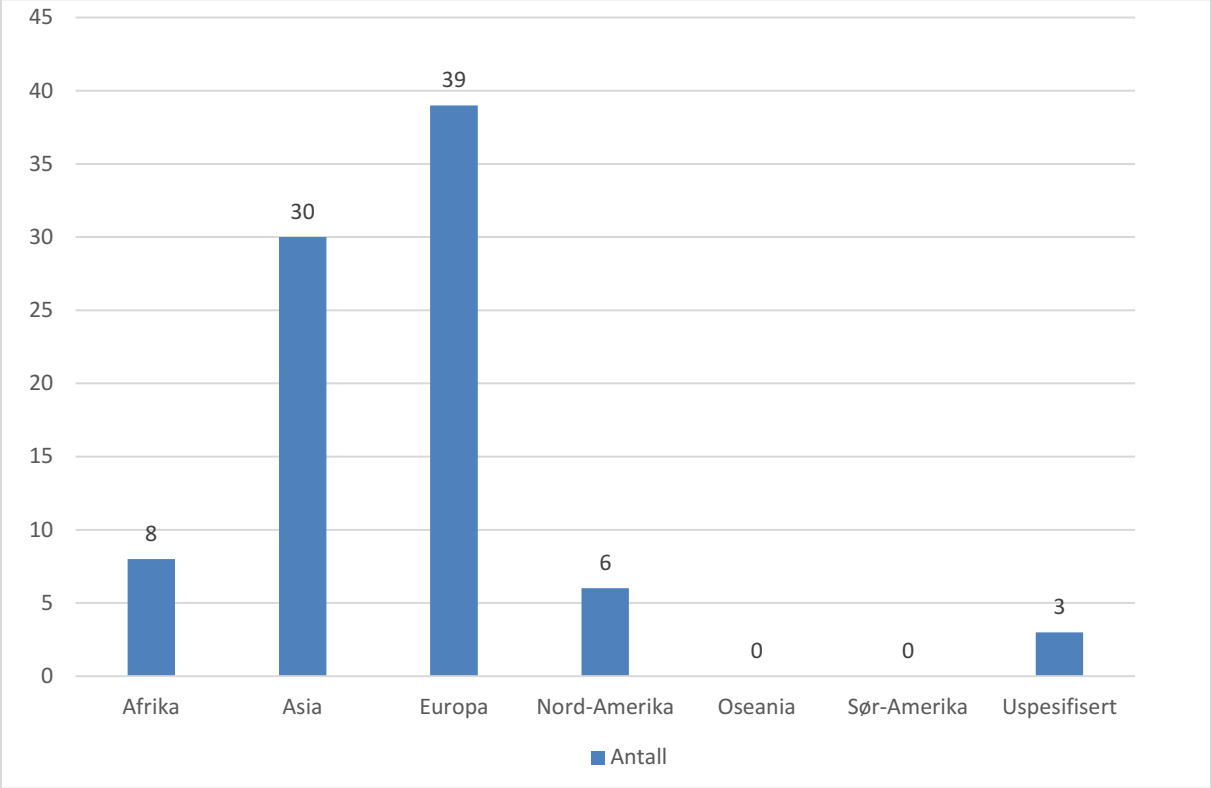
Det er dog tydelig for våre respondenter at det ligger en utfordring i å rekruttere fra disse land. Landene har selv et stort behov for dyktige personer med IKT-sikkerhetskompetanse. Det betyr også at det er en stor risiko for at de personene fra Norden eller Europa og Nord-Amerika som utdannes i Norge, vil reise tilbake til sine hjemland etter endt utdanning, peker flere av våre informanter på.

Det er også rettet et søkelys på et økende antall utenlandsstudenter, spesielt på doktorgradsnivå innen IKT-sikkerhet. Arbeidsnotatet fra fase I av prosjektet viser at det er en betydelig andel. Mange drar hjem etter endt utdanning, og dette vil potensielt forsterke en fremtidig underdekning. Det er derfor interessant å se på hvor utenlandsstudentene kommer fra, noe som kan ha betydning for andelen som forlater Norge etter endt studium.

Figur 6 viser hvordan utenlandsstudentene i IKT-utdanningene som vi identifiserte i fase I av prosjektet, fordeler seg på ulike regioner. Antall studenter er målt langs den venstre vertikale aksen. Figuren viser at nærmere halvparten av utenlandsstudentene i 2016 og 2017 kom fra Vest-Europa. Sannsynligvis er det høyst sannsynlig at denne gruppen forlater Norge etter endt utdanning, ettersom de har et relativt godt arbeidsmarked i sitt hjemland.

[19] Studieavgift omfatter administrative omkostninger knyttet til registering og oppfølging av studentene, og kan i mange tilfeller sidestilles med det som kalles semesteravgift. Deltakeravgift er derimot kurskostnader for deltakerne, disse kan omfatte ulike utgifter knyttet til selve kurset, inklusive lærerkrefter og faglig oppfølging.

Figur 6: Utenlandsstudenter i IKT-sikkerhetsutdanninger fordelt på region. 2016 og 2017.



Kilde: DBH

5.4 «Awareness» et spørsmål om holdningsendring og kultur

Det at Norge er et av verdens mest digitaliserte land er allerede kommentert flere ganger i denne rapporten. Digitaliseringen finner sted i alle lag i samfunnet – og har stor innvirkning på både enkeltindividets liv, hvordan vi utfører jobbene våre og hvordan landet Norge styres. Digitaliseringens hensikt er i bunn og grunn å forenkle ulike prosesser vi tidligere gjorde manuelt eller fysisk,[20] og således påvirker digitaliseringen vi opplever og også tar del i, både vårt daglige liv og virke.

Fordelene ved digitaliseringen er uomtvistelige, og mange (både på individnivå og mer overordnet nivå) har nok omfavnet utviklingen relativt ukritisk. For uomtvistelig kommer digitaliseringen av vår hverdag også med store utfordringer. Og disse utfordringene handler da i første rekke om *sikkerhet*. Hva skjer med informasjonen vi deler med andre via cyber space? Er det sikkert å overføre penger via nett? Osv. Hva vet vi om sikkerhet? Og særlig – hvordan forholder vi oss til spørsmålet om sikkerhet i vår digitaliserte hverdag?

Det ble påpekt i flere av intervjuene vi gjorde at digitaliseringen av Norge har gått så fort at man nærmest har «glemt» å stille enkelte viktige spørsmål i denne prosessen – spørsmål som handler om sikkerhet. Hvor sikre er de nye banktjenestene? Hvor sikkert er det nye lagringssystemet for sykehusets pasientjournaler? Det kan se ut som om digitaliseringskompetansen stort sett ligger et steg foran sikkerhetskompetansen.

Et manglende fokus på sikkerhet dreier seg, slik vi har sett, i stor grad om manglende fokus på utvikling av den rette sikkerhetskompetansen. Men hvorfor har det vært et manglende fokus på kompetansen? Har vi ikke innsett viktigheten av denne kompetansen?

[20] https://snl.no/digitalisering

I en rapport om nordmenn og digital kultur (Norsis - Norsk senter for informasjonssikring, 2017) pekes det på betydningen av flere ulike faktorer som indikatorer på digital sikkerhetskultur. Disse er:

- Fellesskap
- Styring og kontroll
- Tillit
- Risiko-oppfatning
- Optimisme med hensyn til teknologi og digitalisering
- Kompetanse
- Interesse
- Adferdsmønstre

Flere av disse faktorene og betydningen av dem adresseres også av våre informanter. Utgangspunktet for våre intervjuer har vært å belyse behovet for mer kompetanse innen informasjonssikkerhet. Dermed blir selvfølgelig faktoren *kompetanse* relativt behørig belyst i våre intervjuer. Våre informanter er generelt enige om at vi på alle samfunnsnivå har et for avslappet forhold til sikkerhet når det gjelder informasjonsutveksling – vi klarer ikke å stille de rette, kritiske spørsmålene ved sikkerheten når en digitalisert handling utføres. Ifølge våre informanter kreves det nå både et kompetanseløft og en holdningsendring, og for å klare dette er det blant annet en oppfatning om at opplæring i informasjonssikkerhet må inn allerede barnehagen. I den videre skolegangen bør informasjonssikkerhet være et obligatorisk fag på timeplanen.

Fellesskap, styring og kontroll og tillit er også faktorer som blir adressert av våre informanter. For eksempel er det viktig at vi alle, på alle nivå, forstår betydningen av fellesskapet og det kollektive ansvaret for å unngå brister eller huller i informasjonssikkerheten/informasjonsutvekslingen. I et av intervjuene ble det påpekt at «man vil aldri være sterkere enn det svakeste ledd, og at man for eksempel i et næringslivssamarbeid mellom flere aktører vil være avhengig av at aktørene stiller de samme kravene til informasjonssikkerheten». Enkeltindividet representerer også en sårbarhet hva gjelder informasjonssikkerhet, og hver og en av oss har et ansvar for at informasjonssikkerheten i samfunnet ivaretas.

Ett område hvor det er spesielt viktig at enkeltindividet har sikkerhet langt fremme i bevisstheten, er når vi bruker digitale penger. Digitale penger ble nevnt av våre informanter som spesielt utfordrende hva gjelder sikkerhet, og hvor både den enkelte, næringslivet og det offentlige gjør seg sårbare overfor datakriminalitet ved bruk av digitale penger. Og det er ingen tvil om at nordmenn for eksempel er glade i å handle over nettet. Sårbarheten ligger i om vi faktisk vet nok om konsekvensene av å kjøpe klær eller sko eller andre ting over nett. Vet vi at vi legger igjen digitale spor tilbake til oss selv? Tar vi forholdsregler når vi legger inn kredittkortopplysningene? Det er viktig for våre informanter å også presisere at Norge som sådan og også den enkelte nordmann generelt er gode på informasjonssikkerhet, sammenlignet med andre land. Dette er selvfølgelig en konsekvens av at vi er så langt fremme når det gjelder digitalisering av tjenester og oppgaver. Men som alle våre informanter også poengterer, går utviklingen fort, og sikkerhetskompetansen og utviklingen av denne må ligge i forkant av den øvrige utviklingen. Kan noe av bekymringen rundt det opplevde sikkerhetsgapet bøtes på ved å legge til rette for en økt bevissthet rundt informasjonssikkerhet i befolkningen? Vi tolker våre informanter dithen at man gjennom å integrere informasjonssikkerhet som en obligatorisk del av hele vårt utdanningssystem (fra barnehagenivå) vil kunne oppnå noe av dette. Å skulle integrere sikkerhetstenkning som en naturlig del av den norske kulturen, vil selvfølgelig ta tid – enn så lenge handler mye om bevisstgjøring i alle samfunnslag og utvikling av kompetanse.

Imidlertid pekte også enkelte av informantene på at når man diskuterer informasjonssikkerhet, ligger det en utfordring i den utbredte tiltro eller tillit til myndighetene, og at styresmaktene «passer på» eller «ser etter oss». Denne tiltroen er selvfølgelig helt avgjørende for et velfungerende demokrati, og det er heller ingen tvil om at Norge er strengt regulert hva gjelder informasjonsutveksling, for eksempel av

instanser som Datatilsynet. Imidlertid peker informantene på at myndighetene bare kan regulere det som er innfor Norges grenser, og mye informasjonsdeling foregår selvfølgelig på tvers av landegrenser. Og hvem regulerer denne informasjonen? Ifølge våre informanter er dette et viktig spørsmål som alle må ta ansvar for å forholde seg til. I Norge kan vi stole på at styresmaktene alltid har de beste intensjoner for å ivareta landets sikkerhet og den enkeltes sikkerhet, men vi kan ikke nødvendigvis stole på at informasjonssikkerheten blir ivaretatt når vi deler informasjon globalt.

Gjennom intervjuene kom det også frem at det er en endring i *hvem* som håndterer spørsmål rundt informasjonssikkerhet, og i hvilke *fora* slike spørsmål er på agendaen. Flere av informantene kom inn på at man tidligere ofte forbandt spørsmål rundt, og kompetanse knyttet til informasjonssikkerhet, med relativt unge gutter i sorte hettegensere, som også muligens «gravde» seg ned på gutterommet for å dyrke sin lidenskap for data, spill og hacking. Informantene pekte på at man ofte forbandt disse unge guttene med en helt egen kultur, som kanskje også virket ugjennomtrengelig og litt «mystisk». I denne kulturen var det heller ikke plass til kvinner. Men ifølge våre informanter kan det se ut som om denne litt mystiske «hacker-kulturen» er i ferd med å bli mer transparent, hettegenserne byttes ut med blazeren, og det mørklagte gutterommet er byttet ut med styrerommet i en større bedrift. Dessuten påpeker også våre informanter at kvinner i større grad gjør sitt inntog på denne arenaen, og flere av informantene mener selv at de i egen bedrift eller organisasjon har en god kjønnsfordeling hva gjelder sikkerhetskompetanse.

Imidlertid er det slik (noe som også kommer frem i intervjuene) at gjennom at IKT-sikkerhetskompetansen langsomt tar steget ut av gutterommet, gjør behovet for denne kompetansen seg også gjeldende på fagområder som er viktige for eksempel i driftingen av større datasystemer, slik som organisasjons- og ledelsesfag og juss. Informantene er til dels tydelige på at det ofte er innenfor disse områdene at kvinnene per i dag i størst grad gjør seg gjeldende, men at det fremdeles skorter noe på innenfor den mer tekniske delen av utvikling av sikkerhetssystemer og rutine.

5.5 Oppsummerende betraktninger

5.5.1 Metodisk vurdering

Våre intervjuer ble gjennomført blant 18 norske aktører innen IKT-sikkerhet. Vi har søkt å treffe et bredt utvalgt som dekker UH-sektor, forskning, myndigheter, interesseorganisasjoner, og næringsliv. Det er aktører som i de fleste tilfeller har en betydelig egeninteresse i å stille seg ekstra kritiske til dagens situasjon og på den måte søke å «krisemaksimere» og dermed håpe på flere ressurser til arbeidet med IKT-sikkerhet.

Vi er klar over denne mulige bias hos informantene. Derfor søker vi å vurdere flere av utsagnene med informasjon fra andre kilder. Når det for eksempel pekes på at det jobbes med å utjevne kjønnsbalansen og informantene oppfatter balansen som «i bedring», så viser vår gjennomgang av utdanningsstatistikk fra DBH at det ikke er tilfellet.

Omvendt har vi kunnet finne informasjon som støtter opp om de fleste av utsagnene. At det er mangel her og nå på personer med IKT-sikkerhetskompetanse, avspeiles for eksempel i høyt lønnsnivå i stillingsannonser for både nyutdannede og personer med mer erfaring. At EVU-tilbudet er begrenset, er et annet eksempel.

Generelt har vi ikke noen grunn til å betvile synspunktene til våre informanter. De er alle godt informerte aktører innen IKT-sikkerhet. De dekker et mangfold av norske aktører innen IKT-sikkerhet, og likevel peker de relativt unisont på status, utfordringer og mulige løsninger.

5.5.2 Løsninger ifølge våre informanter

Selv om Norge har vært tidlig ute med digitalisering av tjenester og systemer i både offentlig og privat sektor, har vi vist at IKT-sikkerhet ikke alltid har vært like godt ivaretatt. Intervjuene indikerer at

årsakene til denne utviklingen er sammensatte. Mange peker på at en stor utfordring er at man ikke har tatt høyde for IKT-sikkerhet i design og produktutvikling, dette kan skyldes både mangel på kunnskap og kultur. Behovet for slik kompetanse er imidlertid omfattende, og ingenting tyder på at behovet vil bli mindre i fremtiden. Når vi i tillegg også har vist til et stort gap mellom behovet for slik kompetanse og hvor mange som uteksamineres med slik kompetanse, er det grunn til å drøfte ulike måter å løse dette på.

I kapittel 2 har vi sammenfattet og spisset forslag til hvordan kompetansegapet kan fylles på ulike måter. Dette bygger vi på innspill fra informantene supplert med annen informasjon og enkelte egne analyser. Samlet gir dette grunnlag for å peke på følgende tiltaksområder:

1. Øke antallet av kandidater som uteksamineres med IKT-sikkerhetskompetanse. Det gjelder både for de vi i rapporten kaller «generalister» og «spesialister».

2. Det må fortsatt arbeides med å utjevne kjønnsforskjellene. Selv om oppfatningen er at det gjøres en innsats, ser vi at forskjellene øker blant de studerende. Det vil være en idé å øke oppmerksomheten rundt IKT-sikkerhet allerede på videregående skole.

3. Styrke forskningsmiljøene og bygge nye. Det er stor konkurranse om de talentfulle unge som har potensiale til å ta en doktorgrad innen IKT-sikkerhet. En viktig rekrutteringsparameter for disse talentene er at de kommer til å inngå i sterke fagmiljøer. Satse mer på anvendelsesorientert og praksisnær forskning. Ikke bygg forskningsmiljøene utelukkende på grunnlag av tradisjonelle tellekanter, ta også hensyn til muligheten for å videreutvikle samspill mellom kjerneaktører innen feltet (forskning og utdanning og myndigheter/arbeidsliv).

4. Trekke inn flere eksterne undervisere for å imøtegå mangel på undervisere og for å inkludere anvendelsesorienterte og praksisnære perspektiver i utdanningen.

5. Etter- og videreutdanning bør prioriteres. Det vil gi et kompetanseløft på kort sikt, men vil også være relevant på lang sikt for å kunne dekke behov som kontinuerlig skapes av den teknologiske utviklingen. Vi ser at EVU-tilbudet på universitets- og høgskolenivå praktisk talt er fraværende. Det er overraskende all den stund at vi observerer en potensielt stor etterspørsel. Det kan virke som om det er barrierer eller mangel på insentiver for å styrke omfanget. Vi har i dette prosjektet ikke mulighet til å gå i dypere i analysen av dette, men våre informanter knytter det blant annet til utfordringer rundt finansiering. Dette er et område som bør undersøkes nærmere.

For hvert av områdene bør man gå i ytterligere dialog for å kartlegge muligheter og prioriteringer.

6 Behov for IKT-sikkerhetskompetanse i andre land

Det er en global mangel på personer med IKT-sikkerhetskompetanse. Global Information Security Workforce Study (2017) viser at det i 2022 vil mangle opp mot 1,8 millioner personer på verdensbasis som har kompetanse innen IKT-sikkerhet. Med det som bakteppe har vi som en del av rapporten sett på behovet for IKT-sikkerhetskompetanse i andre, sammenlignbare land. Vi har vært interessert i hvordan status for tilbud og etterspørsel er per i dag og hvordan balansen vil se ut i årene som kommer. I tillegg har vi søkt å finne ut hvor høyt spørsmål om IKT-sikkerhet står på den politiske dagsorden og om det er strategier rundt IKT-sikkerhetskompetanse i Sverige, Danmark, Nederland og Storbritannia, alle land som det er naturlig for Norge å sammenligne seg med. Nedenfor følger en kort presentasjon av rasjonale for valg av disse landene, deretter vil vi redegjøre mer utfyllende for hvert enkelt av landene.

- **Sverige** har nettopp offentliggjort en analyse som peker på store kompetanseetterslep innen IKT generelt og IKT-sikkerhet. Våren 2017 kom også en fersk nasjonal digitaliseringsstrategi, og Regeringskansliet arbeider for øyeblikket med en IKT-sikkerhetsstrategi som skal publiseres på et senere tidspunkt.

- **Danmark** har ingen nasjonal analyse eller vurderinger av fremtidens kompetansebehov innenfor IKT-sikkerhet. Det finnes dog en regional kartlegging som dekker Region Hovedstaden. I 2015 ble det gjennomført en kartlegging av viten- og utdanningsaktiviteter innen IKT-sikkerhet. Kartleggingen pekte på hull på utdanningsområdet og at området er sårbart, da undervisning og forskning avhenger av få personer. Den gjeldende strategi er fra forrige regjering, og det er uklart hvordan den nåværende arbeider strategisk med IKT-sikkerhet.

- **Nederland**, her foreligger en forskningsrapport[21] som viser til at det i 2014 var et etterslep på rundt 1 150 personer med IKT-sikkerhetskompetanse. Metoden, basert på stillingsannonser, vil dog gi en betydelig underestimering av det reelle behov, da omfanget av udekkede behov ikke lar seg fullt ut avdekke via dem som rekrutterer gjennom formelle kanaler. Kompetansebehovet innen IKT-sikkerhet er et særskilt fokusområde i den nasjonale IKT-sikkerhetsstrategien.

- **Storbritannia** har etablert en strategi rundt IKT-sikkerhet. Det finnes ikke estimat for nåværende eller fremtidige kompetansebehov, men strategien legger til grunn at det er et betydelig udekket behov for personer med IKT-sikkerhetskompetanse. Frem til år 2021

[21] Rapporten er offentliggjort i 2014.

avsettes i alt 16 000 millioner kroner til å følge opp IKT-sikkerhetsstrategien, som har et klart fokus på å styrke kompetansebasen.

I det følgende beskriver vi disse landende nærmere.

6.1 Sverige

En fersk analyse peker på en betydelig underdekning av behovet for IKT-medarbeidere i Sverige[22] frem mot år 2022. I analysen fremheves 13 sentrale drivkrefter for utviklingen av behovet for medarbeidere innen IKT. Blant de 13 drivkreftene er IKT-sikkerhet, og basert på en survey innenfor svensk næringsliv[23] utpekes IKT-sikkerhet til å være den neststørste drivkraften som påvirker kompetanseetterspørselen. Nærmere 70 prosent av respondentene peker på at IKT-sikkerhet i «høy utstrekning» vil påvirke deres kompetansebehov. I tillegg peker rundt 20 prosent av respondentene på at IKT-sikkerhet i en «viss utstrekning» vil påvirke deres kompetansebehov. Samlet betyr det at rundt 90 prosent av respondentene peker på IKT-sikkerhet som en drivkraft som vil påvirke deres kompetansebehov.

At det allerede i dag er et betydelig underdekket behov i Sverige, bekreftes også av analysen. Her peker analysen på at rundt 15 prosent av respondentene kunne øke antallet medarbeidere med IKT-sikkerhetskompetanse med mer enn 15 prosent, og i tillegg kan rundt 55 prosent av respondentene øke antallet med mellom 5 og 15 prosent.

Analysen ser også på det fremtidige behovet i de kommende 3 til 5 årene. Her peker 25 prosent av respondentene på at de ønsker å øke antallet medarbeidere med IKT-sikkerhetskompetanse med mer enn 15 prosent, og i tillegg kan rundt 60 prosent av respondentene øke antallet med mellom 5 og 15 prosent i de kommende år.

Målt i antall har de 202 organisasjonene som har deltatt i analysen, rundt 5 000 personer ansatt innen IKT-sikkerhet. Da analysen dekker 202 organisasjoner, må de 5 000 personene antas å være betydelig underestimert[24]. Behovet for personer med IKT-sikkerhetskompetanse vurderes til å øke med 35,7 prosent de neste 4 årene. En økning på 35,7 prosent betyr da 1 785 personer ut over de 5 000 som allerede i dag er sysselsatt innen IKT-sikkerhet. Som nevnt må disse tallene antas å være betydelig underestimerte. Sammenholder vi tallene med Norge, estimers det i våre modeller at Norge i 2017 har 8 500 personer sysselsatt innen IKT-sikkerhet. I 2017 vurderes underdekningen i Norge til å være på 2 500 personer.

Våren 2017 presenterte det svenske Regeringskansliet en oppdatering av sin digitaliseringsstrategi. Den forrige var fra 2015. I tillegg til strategien ble det også nedsatt et digitaliseringsråd, som har til formål å støtte gjennomføringen av digitaliseringsstrategien. Innen IKT-sikkerhet har digitaliseringsstrategien følgende punkter:

- Alle må ha en digital identitet slik at de kan delta i en digitalisert hverdag. Denne digitale identiteten må være enkel og sikker.
- Det skal foregå et løpende og systematisk arbeid med sikkerhet, for både enkeltindivider, bedrifter, offentlig sektor og samfunnet. Det arbeides i Regeringskansliet med en egen IKT-sikkerhetsstrategi. Den er imidlertid ikke offentlig ennå.
- Den personlige integritet må ivaretas selv i den digitale utvikling. Det må tas hånd om opplysninger om enkeltindivider.

[22] Se IT-kompetensbristen, IT&Telekomföretagen, Nov 2017
[23] Basert på svar fra 202 respondenter
[24] Bl.a. dekker analysen 4 kommunale enheter og 7 statlige, noe som må antas å bety en betydelig underestimering.

- Demokratiet må vernes i digitale miljøer.
- Overgangen til et stadig mer digitalt arbeidsmarked må skje på en trygg måte.
- Det må være et fokus på å understøtte velfungerende digitale markeder og trygghet for den enkelte forbrukeren.

Strategien har også et fokus på digital kompetanse. Her slås det fast at det er behov for å styrke kompetansenivået innen IKT-området bredt.

Om man skal vær litt kritisk til den svenske strategien, er målene og innsatsene som presenteres, overordnede og vage. Det er lite konkrete tiltak helt generelt, særlig når vi ser på kryssfeltet mellom digital utvikling, IKT-sikkerhet og kompetansebehov. Det er mulig at den kommende strategien for IKT-sikkerhet blir litt mer konkret omkring tiltak på hvordan den svenske regjeringen har tenkt å møte kompetanseetterslepet i Sverige, både innen IKT generelt og særlig da innen IKT-sikkerhet.

6.2 Danmark

Det er en generell holdning at det er mangel på personer med IKT-sikkerhetskompetanse i Danmark. Som i Norge tilbys stort sett alle studerende jobb innen endt utdanning. Det betyr også at det, som i Norge, er vanskelig å få gode kandidater til eksempelvis post doc.-stillinger eller doktorgradsstipendier. Det mangler rollemodeller som kan vise (karriere)veien for andre og skape sterke faglige forskningsmiljøer. Det skaper allerede per i dag den utfordring, at det mangler forskere og undervisere til å utdanne kommende generasjoner med IKT-sikkerhetskompetanse.

Det finnes ikke en nasjonal kartlegging av behovet for personer med IKT-sikkerhetskompetanse. Det finnes dog en regional kartlegging som ble gjennomført tidlig i 2017. Den regionale kartleggingen dekker Region Hovedstaden, som sammen med Region Midtjylland må antas å være de to regionene i Danmark med størst etterspørsel etter personer med IKT-sikkerhetskompetanse.

Kartleggingen bygger på en opptelling av stillingsannonser der det søkes etter spesifikke kompetanser eller kvalifikasjoner innen IKT-sikkerhet. Det kan være: *Cyber security*, *DDos angreb*, *Certified Ethical Hacker*, *databeskyttelse*, *SQL injection* og *sikker it drift*[25]. Tallene viser følgende:

- I 2016 var det 480 stillingsannonser etter personer med IKT-sikkerhetskompetanse. Tallet er på nivå med antallet oppslag fra år 2007, hvor det var 490 stillingsannonser. Som i vår analyse pekes det på en markant nedgang som følge av finanskrisen.
- Forfatterne estimerer på bakgrunn av de 480 stillingsannonsene at det er i alt 850 «jobbåpninger». Det betyr at det i tillegg til de 480 formelle annonsene finnes nesten like mange ledige stillinger som ikke lyses ut via formelle kanaler.
- Tallene viser at IKT-sikkerhet som andel av de samlede stillingsannonsene innen IKT-området i Region Hovedstaden ligger på 5 prosent i 2007, øker til 6 prosent i år 2010, mens andelen deretter faller år for år og ender på 4 prosent i 2016. Fallet må sies å være overraskende all den tid etterspørselen etter personer med IKT-sikkerhetskompetanse antas å øke mer enn det som er tilfellet med IKT generelt[26].
- Ifølge Van Lakerveld et al (2014) anvendes en skaleringsfaktor på 6 for å nå fra antall «jobbåpninger» til det samlede antall sysselsatte innen et område. Det betyr at det er knapt 5 000 personer som arbeider med IKT-sikkerhet i Region Hovedstaden. Og da vil det samlede

[25] Se «Efter spørgslen efter ITsikkerhedsmedarbejdere i Hovedstadsområdet», Højbjerre Brauer Schultz (2017).
[26] I følge ITSVET-PROJECT øker etterspørselen etter personer med IKT-sikkerhet med 3,5 ganger etterspørselen etter personer med IKT-kompetanse generelt.

antallet sysselsatte med IKT-sikkerhetskompetanse skjønnsmessig ligge rundt 8–9 000[27]. Tallene fra våre framskrivninger pekte på at det i 2016 var sysselsatt rundt 8 300 personer med IKT-sikkerhetskompetanse. Men det er selvsagt betydelig usikkerhet forbundet med det, og samtidig sier det lite om fremtidens etterspørsel, ut over at vi historisk kan se, at det har vært økende.

Det finnes som nevnt ikke noe nasjonalt tall for tilbud på og etterspørsel etter personer med IKT-sikkerhetskompetanse. I 2015 utkom en rapport som inneholdt en kartlegging av «viten- og utdannelsesaktiviteter innenfor cyber- og informasjonssikkerhet på danske utdannelses- og forskningsinstitusjoner (Deloitte, 2015). Her ble det kartlagt at alle 8 universiteter samt 5 erhvervsakademier, altså fagskoler, tilbyr IKT-sikkerhetsutdanninger.

Rapporten identifiserer i alt 106 kurs som inneholder et IKT-sikkerhetselement. Samtidig pekes det på områder der dansk forskning utmerker seg. Det gjelder innen kryptologi og andre temaer med fokus på å forhindre cyberangrep med vekt på et matematisk og teknisk grunnlag. Omvendt pekes det på at områder innen databeskyttelse og håndtering når angrepet har funnet sted er begrenset, dette gjelder til eksempel innen *forensics.*

Rapporten peker i tillegg på en sårbarhet innenfor det danske undervisningssystem. Systemet er bygget opp rundt forskningsbasert undervisning. Dette gir en stor avhengighet av en begrenset gruppe mennesker, som både skal forske og undervise. Dessuten er de få personene spredt både faglig og geografisk, noe som gjør det vanskelig å bygge opp fagmiljøer, noe som igjen minsker evnen til å trekke til seg nye kompetanser.

Danmarks nasjonale strategi for cyber- og informasjonssikkerhet ble offentliggjort i desember 2014. Strategien søker å samle kreftene i Danmark og ruste landet mot en stadig økende trussel innen IKT-området. Konkret ledet det til en fortsatt utbygging av Nationalt Cyber Crime Center. I strategien heter det at senteret utbygges slik at det "... *opbygges et stærkt fagligt miljø med specialistfunktioner og særligt avanceret teknologi til understøttelse af efterforskningen af it-kriminalitet*." Dessuten pekes det på at det må skje et kompetanseløft blant etterforskere og i politiet.

På utdanningsområdet anføres det et ønske om å jobbe med å skape et cyber- og informasjonssikkerhetsnettverk. Dette er basert på oppfatningen om at aktivitetene på utdannings- og forskningsområdet innen cyber- og informasjonssikkerhet er relativt fragmenterte. Og samtidig vil man arbeide for å styrke dialogen mellom private og offentlige avtakere av personer med IKT-sikkerhetskompetanse og de som utdanner dem. Den største aktøren innen IKT-sikkerhet er dog Center for Cybersikkerhet. Det bygges opp en del kompetanse i senteret. Senteret har i dag cirka 80 medarbeidere og består av tre avdelinger (Rådgivnings- og Teleavdelingen, Nettsikkerhetsavdelingen og Policyavdelingen).

IKT-sikkerhet står ganske høyt på dagsordenen i Danmark. Dette gjelder i medier og politisk. Likevel virker det som om det på nasjonalt nivå er en slags inerti over IKT-angrep, som eksempelvis angrepet på Mærsk. Skandalesaker rulles opp i media, og politikerne er forarget. Likevel later det ikke til at det kommer noe konkret handling på bakgrunn av det, ut over styrkingen av Center for Cybersikkerhet.

6.3 Nederland

Forskere ved Universitetet i Leiden har gjennomført en kartlegging av arbeidsmarkedet for personer med IKT-sikkerhetskompetanse. Analysen til forskerne fra Leiden er basert på stillingsannonser. Gjennom ett år (fra 4. kvartal 2013 til og med 3. kvartal 2014) identifiseres 1 158 stillingsannonser, der det søkes etter personell med IKT-sikkerhetskompetanse. Det konkluderes samtidig med at den reelle etterspørselen er høyere, da mange ansettes gjennom uformelle stillingsannonser. Den danske

[27] Dette tallet er basert på at rundt 60 prosent av den samlede sysselsetting innen IKT er plassert i Region Hovedstaden, basert på den registerbaserte arbeidsmarkedsstatistikken for årene 2013, 2014 og 2015.

kartleggingen (Højbjerre Brauer Schultz, 2017) konkluderte med at 480 stillingsannonser reelt dekket over rundt 850 jobbåpninger. Om vi anvender samme skaleringsfaktor her, betyr det at det er 2 050 jobbåpninger i Nederland i det tidsrommet analysen dekker.

Antallet personer som jobber med IKT-sikkerhet, anslås til å være 7 000 personer. Det bygger på at det som en tommelfingerregel er én ledig stilling per seks personer som er i jobb innen IKT-området. Dette er dog et tall som øyensynlig er vesentlig underestimert, da det er en underestimering av ledige stillinger (Højbjerre Brauer Schultz, 2017). Til sammenligning viser vår modell og statistikk, presentert i kapittel 3, at det i 2014 er omkring 8 000 personer som jobber med IKT-sikkerhet, og at det er rundt 1 500 ledige stillinger. Da tallene fra Nederland er underestimert, er det vanskelig å gjøre en egentlig sammenligning, men umiddelbart ser det ikke ut til å være så stor avstand mellom tallene.

Samtidig slås det fast at det kommer til å bli en økning i etterspørselen etter personer med IKT-sikkerhetskompetanse i fremtiden. Konkret peker rapporten på at:

> *Two factors keep the work field of the Cyber Security Professional rapidly changing. On the one hand, it is about societal developments (at political, economic, social, technical and judicial level). On the other hand, incidents (depending on the frequency and impact) call for adjustments in the work field.*

Umiddelbart vurderer forskerne at det er tilstrekkelig med utdanningskapasitet i Nederland til å dekke fremtidens behov. De konkluderer med at "*The educational supply regarding cyber security is varied and extensive. Educational programs are often offered on various locations and there is much variation in types of education or training*." Likevel peker de på det er betydelig usikkerhet rundt hvor mange av de omkring 4 500 studerende på minimum bachelornivå som vil ha kompetanse og ønske om å jobbe med IKT-sikkerhet etter endt utdanning. De peker videre også på utfordringen med en skjev kjønnsbalanse blant personer med IKT-sikkerhetskompetanse.

Nederland er et av landene som av våre respondenter er blitt fremhevet som et land med stort fokus på IKT-sikkerhet. Deres nåværende IKT-sikkerhetsstrategi er utarbeidet i 2013 og har 5 strategiske mål:

1. The Netherlands is resilient to cyber-attacks and protects its vital interests in the digital domain.
2. The Netherlands tackles cybercrime.
3. The Netherlands invests in secure ICT products and services that protect privacy.
4. The Netherlands builds coalitions for freedom, security and peace in the digital domain.
5. The Netherlands has sufficient cyber security knowledge and skills and invests in ICT innovation.

I tillegg har man i forbindelse med den forrige IKT-sikkerhetsstrategien nedsatt et råd for IKT-sikkerhet, Cyber Security raad (CSR)[28]. Til slutt kan det nevnes at Nederland har et nasjonalt IKT-sikkerhetssenter, som er organisert under Justis- og beredskapsministeriet.

[28] The Cyber Security Council (CSR) is a national and independent advisory body to the government and is composed of high-level representatives from public and private organizations and science. The CSR is working on a strategic level to increase cyber security in the Netherlands. Due to the unique composition of the board (public-private science) it is possible to strategically approach priorities, bottlenecks and incidents from various angles and to develop an integrated vision of opportunities and threats. The CSR seeks cooperation with similar councils in other countries and encourages their creation in countries that do not yet have a Cyber Security Council.

6.4 Storbritannia

Det finnes ikke umiddelbart noe estimat for samsvaret mellom tilbud på og etterspørsel etter personer med IKT-sikkerhetskompetanse. Likevel er underdekningen av personer med IKT-sikkerhetskompetanse et av omdreiningspunktene for IKT-sikkerhetsstrategien: National Cyber Security Strategy 2016-2021. I strategien slås det fast at:

> *We will use the authority and influence of the UK Government to invest in programmes to address the shortage of cyber security skills in the UK, from schools to universities and across the workforce*". "*The UK requires more talented and qualified cyber security professionals. The Government will act now to plug the growing gap between demand and supply for key cyber security roles, and inject renewed vigour into this area of education and training. This is a long-term, transformative objective, and this strategy will kick-start this important work, which will necessarily continue beyond 2021*.

IKT-sikkerhet er høyt prioritert i Storbritannia og har vært det i flere år. IKT-sikkerhet anses å være en absolutt hjørnestein i det britiske samfunnet. Den nasjonale sikkerhetsstrategien fra 2015 (The National Security Strategi (NSS)) bekreftet IKT-trusler som «… *a Tier One risk to UK interests*». Med andre ord er det en trussel som anses som så betydelig at den potensielt kan skade det britiske samfunnet fundamentalt.

Og videre slås det fast at det mangler IKT-sikkerhetskompetanse på stort sett alle nivåer av det britiske samfunnet. Særlig kritisk er det når det fokuseres på den mer avanserte IKT-sikkerhetskompetansen: "*We also need to develop the specialist skills and capabilities that will allow us to keep pace with rapidly evolving technology and manage the associated cyber risks. This skills gap represents a national vulnerability that must be resolved*."

Målet i strategien er at man blir i stand til å utdanne de dyktigste IKT-sikkerhetstalentene nasjonalt. Dette krever en innsats over ikke bare de kommende 5 år, men de neste 20 årene. For å sikre utdanningen av de beste talentene arbeides det langsiktig med en koordinert innsats mellom regjering, utdanningsinstitusjoner, forskning og næringslivet. Samtidig er det igangsatt spesifikke «her og nå»-intervensjoner som skal forsøke å lukke det nåværende gapet mellom tilbud og etterspørsel. Det nevnes ikke spesifikt i strategien hvilke tiltak det er snakk om.

Tiltakene dekker mange av de tiltakene som også er nevnt i Norge. Det vil si at alle som studerer informatikk, må ha fag innen IKT-sikkerhet. Samtidig vil man ta fatt i kjønnsubalansen som finnes på dette fagområdet. Det gjør man for å sikre en størst mulig pool av tilgjengelig talent. Et tredje tiltak er etablering av programmer på ungdomsskoler og videregående skoler, der interesserte 14–18-åringer får mulighet til å ta utdanning innen IKT-sikkerhet. Det gjelder klasseromsundervisning, etter skoletid-sesjoner med eksperter og mentorer samt sommerskoler.

Den omfattende strategien bakkes opp av en betydelig finansiering. Den forrige IKT-sikkerhetsstrategien, for tidsrommet 2011–2016, ble finansiert med 7 200 millioner kroner. Det beløpet er markant økt i den nye strategien, som finansieres med mer enn 16 000 millioner kroner, godt 3 000 millioner kroner om året. Det representerer med andre ord godt og vel en fordobling, noe som tydelig indikerer at IKT-sikkerhet er høyt på dagsordenen i Storbritannia.

Det er ikke alle midlene som knyttes opp mot utdanning og utdanningstiltak. Senter for IKT-sikkerhet (National Cyber Security Centre) har blitt etablert med midler fra strategien, på samme tid som det er avsatt 1 400 millioner kroner til et innovasjonsfond for IKT-sikkerhet. I Storbritannia ser man store muligheter i å utvikle og bygge opp et næringsliv rundt IKT-sikkerhet.

6.5 Oppsummering

Det er gjennomgående for de fire landene at IKT-sikkerhet og -kompetanse er på dagsordenen. Om enn det er forskjell i hvor langt de enkelte landene har gått i å tallfeste behovet for IKT-sikkerhetskompetanse, er det opplagt et fokusområde.

Både i Danmark og Nederland har man brukt stillingsannonser som kilde til å tallfeste behovet for personer med IKT-sikkerhetskompetanse. Det viste en manko på henholdsvis 480 personer i Region Hovedstaden i 2016 og 1 158 i Nederland i 2013. Dette er tall som er mindre enn de vi finner i Norge, men tall som samtidig åpenbart er underestimert. Den danske rapporten (Højbjerre Brauer Schultz, 2017) peker på at den reelle manko er rundt 850 personer og da alene dekkende for Region Hovedstaden. Den nederlandske rapporten gjør ikke noe estimat, men konstaterer at 1 158 underestimerer den reelle etterspørselen.

I Sverige har man anvendt en blanding av spørreskjema og yrkeskategorisering via registerdata. Via registerdata vises det at om lag 1 400 personer per i dag har en yrkeskategori som kategoriseres som værende innen IKT-sikkerhet. Tallet virker lavt, og i et gjennomført spørreskjema påpeker 202 svenske bedrifter, at de samlet har rundt 5 000 IKT-sikkerhetspersoner ansatt. Hva det samlede tallet for Sverige er, kan være vanskelig å spå om, men det må konkluderes med at rundt 5 000 personer med IKT-sikkerhetskompetanse er et underestimat.

Det ser dog ut til at antallet sysselsatte personer med IKT-sikkerhetskompetanse i de fire landene er på et noenlunde ensartet nivå. Et skjønnsmessig estimat for Danmark er 8–9 000 personer, for Nederland er tallet høyere, basert på et høyere antall stillingsannonser, og tallet for Sverige er minimum 5 000, og antakelig betydelig høyere, når det sammenholdes med Norges estimerte 8 300 sysselsatte personer med IKT-sikkerhetskompetanse[29]. Samlet gir det et inntrykk av et noenlunde likt nivå på tvers av land.

Felles for landene er utfordringene med at digitalisering og bruken av IKT inngår i alles hverdager. Samtidig pekes det på at den teknologiske utviklingen går fort, og med mindre det gjøres en aktiv innsats, åpner utviklingen opp for omfattende sikkerhetshull. Dette gjelder både for den enkelte borger, i næringsliv og offentlig sektor. For å møte denne utfordringen peker de fleste landene, med unntak av Sverige, på at det må skje en utvikling i den nasjonale kompetansebasen. I Sverige holder man på med å utarbeide en nasjonal IKT-sikkerhetsstrategi. Det er rimelig å anta at den vil adressere kompetansebehovet.

I de nasjonale strategiene er det konsensus omkring det intensjonelle. Vi må gjøre noe i forhold til de økende sikkerhetsmessige utfordringene. Så langt ser det ut til at det hovedsakelig er Storbritannia som setter virkelig handling bak intensjonene. Her er man konkret i forhold til mål, aktiviteter og ressursallokering til de forskjellige initiativer. Det er derfor en idé å se mot Storbritannia for inspirasjon til konkrete aktiviteter og hvordan disse er implementert. Samtidig er Storbritannia det eneste av landene som fremhever de næringsmessige mulighetene, som ligger i å kunne tilby troverdige og robuste IKT-sikkerhetssystemer. Det bør også være noe som Norge kan la seg inspirere av.

[29] Det eksakte tall vil dog være lavere enn tilbudssiden, da ikke alle vil være tilgjengelige for arbeidsmarkedet av den ene eller andre årsak, for eksempel permisjon, sykefravær eller migrert.

Vedlegg

Appendiks: Metode kvantitativ framskrivning

Analysen bygger på Statistisk sentralbyrås (SSB) framskrivinger av tilbud på og etterspørsel etter samtlige utdanningsgrupper i Norge. Følgelig er framskrivningene i tråd med andre framskrivninger med fokus på tilbud på og etterspørsel etter kompetanse målt i utdanningsnivå og utdanningsretning i det norske arbeidsmarked. Statistisk sentralbyrå benytter den makroøkonomiske modellen MODAG til å framskrive etterspørselen og mikrosimuleringsmodellen MOSART til å beregne tilgangen på kompetanse, se eksempelvis Holmøy m.fl. (2014) og Dapi m.fl. (2016).

Målet for denne studien er å vurdere mulige fremtidige gap mellom tilbud på og etterspørsel etter IKT-sikkerhetskompetanse i Norge. Det har i løpet av de siste årene blitt utviklet framskrivningsmodeller i mange land for å skaffe seg kunnskap om behovet for ulike typer arbeidskraft i framtiden. Wilson m.fl. (2004) gir en oversikt over disse og konkluderer med at «beste praksis» er å benytte en makroøkonomisk modell med flere næringer, slik at man kan ta hensyn til at næringsendringer påvirker behovet for arbeidskraft med ulik kompetanseprofil. Denne studien er likeledes brutt ned på næringsnivå, tallene inneholder dog en del usikkerhet og offentliggjøres derfor ikke. Deretter summerer vi resultatene opp til et samlet samfunnsnivå og kan dermed gi et estimat på eventuelle fremtidige gap.

Modellene som benyttes, inneholder derfor ofte en såkalt kryssløpskjerne som ivaretar samspillet mellom de ulike næringene gjennom såkalte input-output-relasjoner. Input-output-relasjoner beskriver hvordan produkter og tjenester i én næring er innsatsfaktorer i en annen næring, og hvordan prisen på de ulike produktene og tjenestene avhenger av hvordan de brukes. Dermed framskrives sysselsettingen innenfor hver næring på en måte som følger av endring og utvikling i næringslivet og offentlig sektor. Dermed blir modellene også konsistente med endringer som skjer i næringslivet og offentlig sektor, noe som er en opplagt styrke ved denne typen modeller.

Det er også en styrke ved denne modelltypen at den åpner for å legge inn alternative forutsetninger for framskrivningene. Det betyr at det er mulig å justere på bakgrunn av historiske forutsetninger dersom vi ønsker et annet utgangspunkt for framskrivningene – eventuelt kan vi justere på utviklingshastigheten i framskrivningene. Dette kan baseres på oppdatert statistikk, informasjon om faktiske forhold, om endring i policy eller den økonomiske politikken.

I Norge har det eksistert et modellsystem for framskrivning av behovet for ulike typer arbeidskraft i tråd med dette siden 1993. Opplegget er basert på Statistisk sentralbyrås makroøkonomiske modell MODAG. Det gir grunnlag for at de beregnede tallene for etterspørselen kan sammenholdes med resultatene fra mikromodellen MOSART, som beregner den sannsynlige tilgangen på arbeidskraft etter utdanning.

I utgangspunktet har det vært lagt til grunn at sysselsettingens sammensetning etter utdanning utvikler seg i tråd med trender observert i de foreliggende årene. Denne tilgangen har tidligere blitt benyttet av SSB med noe ujevne mellomrom, og resultater ble publisert i Bjørnstad m.fl. (2010) og Cappelen m.fl. (2013). Beregningene for disse modellene strekker seg fram til 2030.

Appendiks: Introduksjon til MODAG

MODAG er Statistisk sentralbyrås makroøkonomiske modell for framskrivinger av norsk økonomi. Modellen benyttes til framskrivninger og politikkanalyser for sentrale størrelser i økonomien. Finansdepartementet er hovedbruker av modellen, men modellen brukes også av Statistisk sentralbyrå til egne analyser og til analyser på oppdrag for andre. Modellen skiller mellom om lag 45 produkter og 21 næringer, og spesifiserer et stort antall sluttanvendelser av produktene. Videre differensieres produktene på priser avhengig av tilgang (norsk- eller utenlands produsert) og anvendelse (eksport- eller hjemmemarkedet). Modellen er bygget opp av rundt 4000 likninger.

Framskrivning av arbeidskraftsbehov er relativt ensartet, siden arbeidsmarkedet kun er delt i fem utdanningskategorier. Til gjengjeld er næringsstrukturen relativt rikt beskrevet. MODAG kan derfor gi en fyldig beskrivelse av hvordan endringene i næringsstrukturen påvirker den samlede arbeidskraftsetterspørsel, men MODAG kan ikke i seg selv beskrive hvordan næringsutviklingen påvirker etterspørselen etter detaljerte utdanningsretninger. For å gjøre dette har Statistisk sentralbyrå beregnet andeler av sysselsettingen i hver enkelt næring og for hver enkelt av disse fem utdanningskategoriene historisk, og deretter framskrevet andelene trendmessig. Ved å multiplisere de framkomne andelene med sysselsettingen ifølge modellprognosene, har man også kunnet lage anslag for sysselsettingen etter detaljerte utdanningsretninger.

I denne studien anvendes en tilsvarende næringsandelsmetode. Vi bygger på estimater etablert i rapporten om «Dimensjonering av avansert IKT-kompetanse», DAMVAD og Samfunnsøkonomisk Analyse (2014). Næringsandelsmetoden bygger på hvor mange ansatte med en gitt kompetanse (her målt på utdannelsesretning og nivå), som er ansatt innen en gitt næring, samt den forventede.

For å framskrive behovet for IKT-sikkerhetskompetanse har også vi benyttet en slik «næringsandelsmetode». Denne baserer seg på opplysninger om hvor mange personer med de relevante utdanningene som er ansatt innenfor hver av de ulike næringene i norsk økonomi, samt opplysninger om forventet utvikling i disse næringene. Etterspørselen kan dermed beregnes på følgende måte:

$$N_t^{IKT} = \sum_i \sum_k a_{i,k,t}^{IKT} * N_{i,k,t} \qquad (1)$$

Det enkelte element i ligning (1) viser da:

- *i* er ulike næringer
- *k* er ulike utdanningsgrupper
- *t* angir årstall
- $a_{i,k,t}^{IKT}$ er andelen med IKT-sikkerhetskompetanse i næring *i* innenfor utdanningskategori *k* i år *t*
- *N* er samlet sysselsetting
- N^{IKT} er sysselsetting av personell med IKT-sikkerhetskompetanse

$a_{i,k,t}^{IKT} * N_{i,k,t}$ viser dermed antall IKT-sikkerhetsutdannede innen utdanningsretning *k* i næring *i*. Det første summetegnet summerer næringer, og det andre summerer utdanningsretninger. Dermed får vi et estimert total tall for antall sysselsatte med IKT-sikkerhetskompetanse.

Dataene for $N_{i,k,t}$ framover i tid har vi fra underlagsmaterialet til Bjørnstad m.fl. (2010) og DAMVAD og Samfunnsøkonomisk Analyse (2014). Disse sysselsettingstallene er framskrevet sammen med den makroøkonomiske utviklingen som fremkommer i MODAG.

Verdier for $a_{i,k,t}^{IKT}$ er framskrevet på bakgrunn av et estimat basert på beregninger i DAMVAD og Samfunnsøkonomisk Analyse (2014). I den rapporten ble faktisk antall sysselsatte med IKT-utdanning i perioden 2000-2010 identifisert via registerstatistikk[30] fra Statistisk sentralbyrå.

Appendiks: Introduksjon til MOSART

For å framskrive tilbudet av IKT-sikkerhetskompetanse anvendes MOSART. MOSART benytter individuelle kjennetegn, og på bakgrunn av dette beregnes sannsynlige valg knyttet til utdanning og

[30] BHU-registeret som viser befolkningens høyeste fullførte utdanning, med AA-registeret, som viser hvilken næring de er sysselsatt i.

arbeidsmarkedstilknytning for hvert enkelt individ. Disse valgene for hvert enkelt individ blir simulert ved tilfeldige trekninger av begivenheter. Begivenhetene omfatter inn- og utvandring, død, fødsler, pardannelse og -oppløsning, husholdningstilknytning ellers, skolegang og innvirkning på utdanningsnivå, pensjonering, arbeidstilbud og -inntekter samt et enkelt inntektsregnskap på individnivå. På utdanningssiden tar individene følgende beslutning:

- Om de skal starte en utdanning
- Hvilket utdanningsnivå og utdanningsretning de skal velge
- Om de skal fullføre utdanningen
- Om de skal fortsette utdanningen

Sannsynlighetene for ulike utfall avhenger av kjennetegn ved individet selv, for eksempel sannsynligheten for å ta fatt på en høyere utdanning når individet er kvinne og nettopp har fullført videregående skole. Det er opplagt at økonomiske forhold som framtidig avlønning og arbeidsledighet kan spille en rolle for utdanningsvalg og arbeidsmarkedstilknytning. Dette er direkte inkludert i modellen, og for å imøtekomme dette er det valgt en lengre periode for å tallfeste overgangssannsynlighetene i utgangssituasjonen. Da vil de i så liten grad som mulig være påvirket av konjunktursituasjonen.

Estimeringen av tilbudet av IKT-sikkerhetskompetanse følger DAMVAD og Samfunnsøkonomisk Analyse (2014). Her fremskrives tilbudssiden ved å holde andelene i de ulike utdanningsgruppene konstante på 2010-nivå og multiplisere med antallet totalt i gruppene ifølge framskrivingene i Cappelen m.fl. (2013). Matematisk uttrykkes dette slik:

$$NT_t^{IKT} = \sum_k b_{k,2010}^{IKT} * NT_{k,t} \qquad (2)$$

De enkelte elementene i ligning (2) viser da:

- *k* er ulike utdanningsgrupper
- *t* angir årstall
- $b_{k,2010}^{IKT}$ er andelen IKT-utdannete innenfor utdanningskategori *k* i 2010
- N^{IKT} er totalt antall personer med IKT-sikkerhetskompetanse

$NT_{k,t}$ er totalt antall personer med utdanning innenfor utdanningsgruppe *k* i år *t* ifølge Cappelen m.fl. (2013).

Appendiks: Tolkning av resultater

Vi omtaler framskrivingene som både tilbud og etterspørsel etter personell med IKT-sikkerhetskompetanse. Det gjør også Statistisk sentralbyrå i sine framskrivinger av kompetansebehov og tilbud. Der er dog visse forbehold som må gjøres, da en slik tolking ikke er helt presis. Det er nødvendig å klargjøre hva framskrivingene faktisk viser og hvilke forutsetninger de bygger på.

Etterspørselen er basert på tall over faktisk sysselsetting og ikke et underliggende behov som finnes i næringslivet og offentlig sektor. Det kan være mange grunner til at faktisk sysselsetting avviker fra behov. For eksempel kan det være ønske om å ansette flere personer med en gitt utdanning, men siden det ikke er flere i markedet, får man ikke fylt de ledige stillingene. Alternativt ansettes personer med en ikke adekvat utdanning, men som allikevel vurderes å kunne dekke den etterspurte kompetansen. I MODAG er det mulig å gjøre kvalitative tilpasninger, som vi skal se i kapittel 3.3. Men i utgangspunktet, det vil si i det som vi kaller basisscenariet, kapittel 3.4, vil ikke MODAG fange opp eventuelle underliggende behov.

Den observerte sysselsettingen finner sted til gjeldende lønnsnivå. Det er ikke sikkert at så mange innenfor en utdanningsgruppe hadde blitt sysselsatt dersom lønnsnivået hadde vært høyere. Da hadde det vært for dyrt for arbeidsgiver. Siden framskrivningene på etterspørselssiden er basert på den historiske utviklingen, betinger resultatene at lønnsforskjellene holder seg frem til år 2030. Det gjelder både lønnsforskjellene mellom ulike utdanningsgrupper og bedriftenes inntjening, slik at de ikke går med underskudd. Endres lønnsforskjellene, vil det trolig oppstå ønske om å substituere seg bort fra arbeidskraften som har blitt dyrere. Dette er selvsagt en sterk antakelse i MODAG-modellen.

På tilbudssiden bygger tallene på observerte personer med en gitt utdanning. Vi baserer tallene på et faktisk antall med en gitt utdanning. Dette knytter seg til oppdelinger på formelt utdanningsnivå og inkluderer ikke etter- og videreutdanning, kompetanse i arbeidslivet eller selvlært kompetanse.

Framskrivningene bygger på forventet endret antall basert på beregnet sannsynlighet for at det enkelte individ velger nettopp en utdanning innen IKT-sikkerhet og at de gjennomfører den. Her spiller selvsagt en rekke faktorer inn på validiteten. Det kan eksempelvis være at antallet av studieplasser økes betraktelig, at flere ønsker å ta en utdanning innen IKT-sikkerhet og at gjennomføringsgraden økes. Framskrivningen av tilbudssiden tar også inn over seg inn- og utvandring, noe som kan være vanskelig å fremskrive, da det blant annet avhenger av internasjonalt tilbud og internasjonal etterspørsel. Alle disse er faktorer som i løpet av få år kan endre fundamentet for de beregnede sannsynligheter og dermed påvirke framskrivningen.

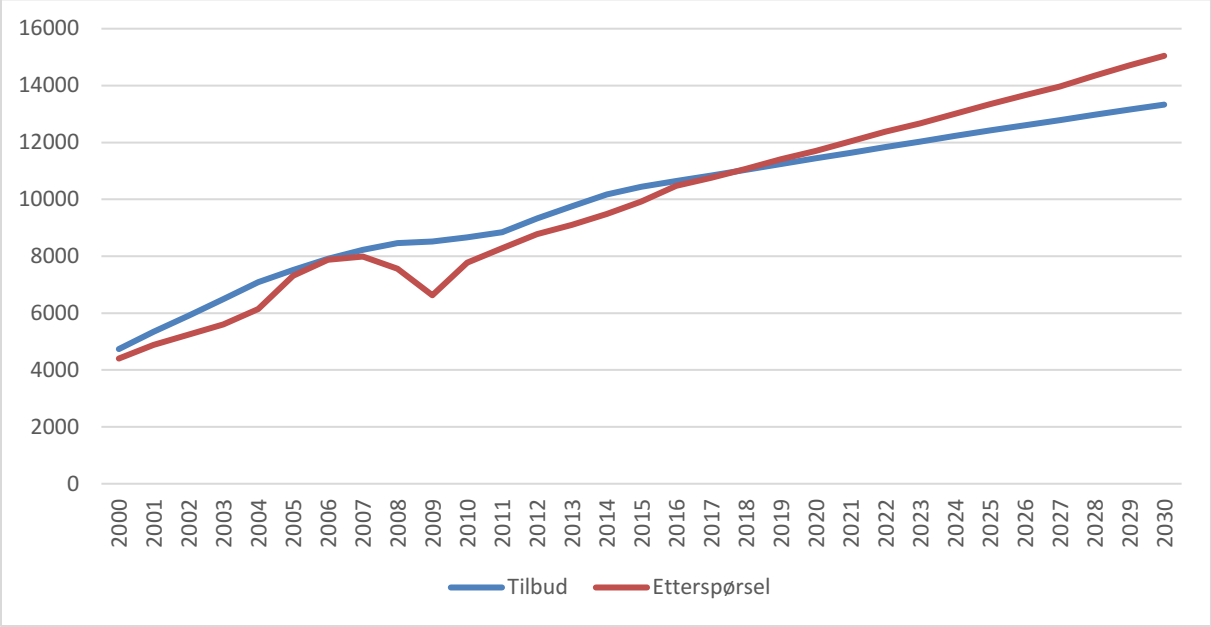
Appendiks: Basisframskrivning

Figur 2 viser vi tilbud på og etterspørsel etter personell med IKT-sikkerhetskompetanse under forutsetning av flere kvalitative vurderinger. Dersom vi ikke gjør disse kvalitative vurderingene, får vi et scenario som viser fremtidig tilbud og etterspørsel basert alene på MOSART- og MODAG-modellene. Med andre ord får vi et slags basisscenario.

Figur 7 viser framskrivning av tilbud på og etterspørsel etter personell med IKT-sikkerhetskompetanse. Figuren viser at frem til år 2015-2016 overstiger tilbudet etterspørselen. Dette er som forventet, da vi i modellene bygger på faktiske tall basert på registerbasert arbeidsmarkedsstatistikk. I slike statistikker vil tilbudet på en bestemt utdanningsgruppe generelt ligge over etterspørselen. Dette skyldes at det alltid vil være personer som av en eller annen grunn er utenfor arbeidsmarkedet. De vil imidlertid fremdeles telle med i statistikken på tilbudssiden. Omvendt vil etterspørselssiden avspeile personene som er i jobb med den gitte utdanningen. Det er kun en indikasjon på etterspørselen. Statistikken vil da ikke fange opp tilfellene der arbeidsgiver har måttet ansatte personell uten IKT-sikkerhetskompetanse i stillinger rettet mot IKT-sikkerhet. I tillegg fanger heller ikke statistikken opp tilfeller der arbeidsgiver har måttet gi opp å ansette personell med IKT-sikkerhetskompetanse.

Framskrivningen i figur 7 viser at det fremdeles vil være mangel på personell med IKT-sikkerhetskompetanse i år 2030. Konkret viser modellen at det vil mangle 1 715 personer i år 2030. Dette svarer til et underskudd på rundt 16 prosent. Selv om estimatet viser et mindre underskudd på personell i år 2030, så viser framskrivningen dog fortsatt at det vil være mangel på personell med IKT-sikkerhetskompetanse i år 2030.

Figur 7: Basisscenario tilbud og etterspørsel etter personell med IKT-sikkerhetskompetanse



Kilde: NIFU 2017

Appendiks: Metode og informantgrunnlag ved intervjuer

Ulike nivå for datainnsamling – makro- og mesonivå

For å belyse ulike aktørers vurdering av IKT-sikkerhet, har vi involvert informanter på to nivå, meso- og makronivået. Samlet sett har vi intervjuet 18 ulike norske aktører, samt vært i dialog med aktører fra fire utvalgte land.

Makronivået omfatter myndighetsnivået, og her inngår informanter fra departement og forvaltning. På mesonivået har vi intervjuet personer tilknyttet universitets- og høgskolesektoren, herunder personer tilknyttet studieprogram om IKT-sikkerhet og informanter tilknyttet særskilte kompetansemiljø innenfor IKT-sikkerhet. Mesonivået omfatter også private selskaper og organisasjoner. De følgende avsnittene beskriver nærmere våre informantgrupper knyttet til de to nivåene.

Vi utviklet intervjuguider tilpasset de ulike informantgruppene, og informantene ble kontaktet med forespørsel om å delta via e-post. Vi oversendte tema for intervjuet i forkant. Resymé fra intervjuene ble oversendt informantene for verifisering.

Makronivået – intervju med ulike myndighetsaktører

Vi intervjuet representanter for Kunnskapsdepartementet, Justis- og beredskapsdepartementet, Helsedirektoratet, Difi og UNINETT AS. Disse informantene har på hver sitt vis bidratt til å belyse ulike sider knyttet til myndighetenes arbeid rundt IKT-sikkerhet. Nedenfor følger en kort presentasjon av informantene og rasjonalet for å bidra til studien.

Justis- og beredskapsdepartementet (JD) har en pådrivende rolle innenfor IKT-sikkerhet, departementet sender ut føringer og arrangerer tverrsektorielle øvelser, samt gir nasjonale føringer til alle departementene og ber dem følge opp etatene igjen. Departementet har en samordning for IKT-sikkerhet på sivilsiden, målet er å skape et helhetlig bilde på tvers av sektorer rundt IKT-sikkerhet, ved å øke kunnskapen.

Kunnskapsdepartementet (KD) har IKT-sikkerhetskompetanse høyt på agendaen. Man har tatt utgangspunkt i problemstillingene som Lysneutvalget pekte på når det gjelder kompetanse. Det er opprettet samarbeid med flere departementer (blant annet Kommunal- og

moderniseringsdepartementet og Justis- og beredskapsdepartementet) hva gjelder IKT-sikkerhet. Er også jevnlig i kontakt med UHR (Universitets- og høgskolerådet) når det gjelder gjennomgang av aktuelle utdanninger.

Difi ligger under Kommunal- og moderniseringsdepartementet. Sikkerhet omfattes i hovedsak av to miljøer: 1) id-porten og 2) kompetansemiljø for informasjonssikkerhet som bistår andre offentlige institusjoner (helseforetak, fylkesmann, andre departementer osv.).

Helsedirektoratet, Utvikling og forvaltning og herunder en divisjon som heter Digital utvikling i Helsedirektoratet. Denne utvikler applikasjoner, programvarer og IKT-systemer for helsesektoren. Interne IKT-tjenester, Vi deler ofte området vårt inn i to; Helseforvaltning og helserefusjon. EHelse har ansvar for de nasjonale løsningene i helsetjenesten.

UNINETT AS er et selskap som er 100 prosent eid av Kunnskapsdepartementet (KD). UNINETTs primærvirksomhet er forskningsnettet, som er koblet opp til universiteter og høgskoler. Selskapet har ansvar for felles anskaffelser i sektoren, blant annet Feide, Eudroam, plagiatkontroll og ansvaret for digitale læringsplattformer. Informanten var leder for informasjonssikkerhet i UH-sektoren.

Mesonivået: intervju med private bedrifter, bransje- og interesseorganisasjoner og UH-miljø

Mesonivået omfatter intervjuer med informanter fra bedriftene Telenor og ATEA, bransje- og interesseorganisasjonene IKT Norge, Abelia, LO og Tekna samt UH-miljø som på ulike måter arbeider med IKT-sikkerhet som Simula, HiOA, NTNU og Sintef.

Telenor er et av Norges største konsern målt etter sysselsetting. Statens eierandel i Telenor er 54 prosent gjennom Nærings- og fiskeridepartementet og 4 prosent gjennom Statens pensjonsfond. Telenor betjener ca. 150 millioner mobilkunder i Europa og Asia (wikipedia.no). Informanten til vår studie arbeidet med sikkerhetsstyring og personvern i Norge.

Atea finnes i syv land i Norden og Baltikum, har ca. 6 800 medarbeidere, er markedsleder i Norden og Baltikum og er den tredje største IT-infrastrukturleverandøren i Europa.

IKT-Norge er en interesseorganisasjon for norske IKT-bedrifter som jobber for økt IT-anvendelse i Norge. Medlemmene er i stor grad større nasjonale og internasjonale IKT-bedrifter. IKT Norge holder i dialogen med leverandører og gir uttrykk for tydelige forventninger og retningsutpeking om hvordan bruke teknologien. IKT-sikkerhet er også ivaretatt som et politisk tema.

Abelia er en av 17 landsforeninger i NHO og retter seg hovedsakelig mot bedrifter innen teknologi og kunnskap, men også en del andre medlemsbedrifter/organisasjoner fra andre sektorer. Ca. 2000 medlemsbedrifter og 48 000 årsverk. IKT-bedrifter utgjør i overkant av 40 prosent av medlemsmassen.

LO har ansvar for samfunnsliv og politisk liv. LO har 1 million medlemmer, de er igjen medlemmer i 26 ulike fagforbund. LO er en hovedorganisasjon, og dens oppgave er å koordinere arbeidet til de 26 forbundene. Næringspolitisk avdeling er en stor avdeling med 16 ansatte som har forskjellige ansvarsområder, herunder digitalisering.

Tekna er Norges største akademikerforening, representerer over 73 000 medlemmer, herav rundt 12500 medlemmer som befatter seg med IT-virksomhet.

Simula@UiB er et frittstående forskningssenter med særlig fokus på kryptologi, datasikkerhet og IT-teori.

SINTEF er et oppdragsforskningsinstitutt, og innenfor informasjonssikkerhet har de mye EU- og Forskningsrådsprosjekter, blant annet sammen energisektoren.

Center for Cyber and information Security, NTNU – campus Gjøvik. Størst i Skandinavia på informasjonssikkerhet. Forsker på relevante problemstillinger og har mange samarbeidspartnere (blant

andre Forsvaret, Telenor) fordi man ønsker å bygge langsiktige, bærekraftige forskningsmiljøer som vokser. Har utdannet ca. 500 kandidater siden 2002 og frem til nå (bachelor, master, ph.d.).

Institutt for datateknologi og informatikk (IDI), NTNU, har to studieprogram som omfatter IKT-sikkerhet: et program i datateknologi og master + bachelor i informatikk + masterprogram i sivilingeniør.

Oppsummering og vurdering av datagrunnlag

Nedenfor har vi oppsummert makro- og mesonivået, datakilder og informantgrunnlag.

Tabell 8 Datakilder og informanter

Makro	
Justis- og beredskapsdepartementet	Myndighet
Kunnskapsdepartementet	Myndighet
Kommunal- og moderniseringsdepartementet	Myndighet
Difi	Myndighet
Helsedirektoratet	Myndighet
Uninett	Myndighet (KDs sektorpolitiske organ for forskningsnett)
Oslo Kommune	Myndighet
Meso	
Telenor	Bedrift
Atea	Bedrift
IKT Norge	Bransje- og interesseorganisasjoner
Abelia	Bransje- og interesseorganisasjoner
LO	Bransje- og interesseorganisasjoner
TEKNA	Bransje- og interesseorganisasjoner
SIMULA senter IKT sikkerhet	UH-sektor, Forskningssenter
CCIS	UH-sektor, forskningssenter
Sintef-Digital	UH-sektor
Utdannings- og forskningssenter for digitalisering (HiOA)	UH-sektor
NTNU, Institutt for datateknologi og informatikk	UH-sektor

Studien støtter seg på et omfattende intervjumateriale der ulike informantgrupper er godt representert. Opprinnelig hadde vi ønske om å inkludere ytterligere flere informanter, som for eksempel Nasjonal sikkerhetsmyndighet, Universitetet i Oslo og Statoil, men dette lot seg dessverre ikke gjennomføre siden det ikke var tid til flere påminnelser om våre henvendelser innenfor prosjektets begrensede tidsrammer. Vi mener likevel å ha et godt datagrunnlag for å kunne besvare spørsmål og problemstillinger som ligger til grunn for denne studien. Vi har mer enn én informant og ofte mange informanter innenfor både makro- og mesonivået og innenfor mesonivået også innenfor underliggende kategorier.

Internasjonale intervjuer og kontakter

I tillegg til de norske respondentene har vi vært i kontakt med og drøftet dagens status og fremtidens behov for IKT-sikkerhetskompetanse i fire utvalgte land. Dessuten har vi bedt våre kontakter om å identifisere forskning eller analyser om fremtidens behov for IKT-sikkerhetskompetanse og hvor høyt IKT-sikkerhet rangerer på den politiske dagsordenen i det enkelte land. Nedenfor er det en oversikt over personer, som vi har vært i dialog med.

Tabell 9 Datakilder og informanter

Land	Person
Sverige	Fredrik von Essen, näringspolitisk expert, IT&Telekomföretagen
Danmark	Christian D. Jensen, ass. professor, DTU
Nederlandene	Dutch National Cyber Security Centre, Drs Zonneveld, dear Dr. Lakerveld begge Plato, Leiden University
Storbritannia	The National Security Secretariat, part of Cabinet Office

Referanser

Bjørnstad, R., Gjelsvik, M. L., Godøy, A., Holm, I., & Stølen, N. M. (2010). *Demand and supply of labor by education towards 2030 - Linking demographic and macroeconomic models for Norway.* Oslo–Kongsvinger: Statistisk sentralbyrå.

Cappelen, Å., Gjefsen, H., Gjelsvik, M., Holm, I., & Martin, S. N. (2013). *Forecasting demand and supply of labour by education.* Oslo–Kongsvinger: Statistisk sentralbyrå .

DAMVAD. (2013). *Intergrating Global Talent in Norway.* Oslo: DAMVAD.

DAMVAD, & analyse, S. (2014). *Dimensjonering av avansert IKT-kompetanse.* Oslo: Kommunal og Moderniseringsdepartementet.

Dansk Teknologisk Institut, & Fraunhofer. (2012). *e-Skills for Cloud Computing, Cyber-security and Green IT - A call for Action.* DG Enterprise and Industry.

Dapi, B., Gjefsen, H. M., Sparrman, V., & Stølen, N. M. (2016). *Education-specific labour force and demand in Norway in times of transition.* Oslo–Kongsvinger: Statistisk sentralbyrå.

Deloitte. (2015). *Kortlægning af viden- og uddannelsesaktiviteter inden for cyber- og informationssikerhed på danske uddannelses- og forskningsinstitutioner.* København: Styrelsen for Forskning og Innovation.

Department for Business Innovation and Skills. (2014). *Cyber Security Skills - Business perspectives and Government's next steps.* London: Department for Business Innovation and Skills.

Direktoratet for forvaltning og IKT. (2012). *Styringssystem for informasjonssikkerhet - Erfaringer med og anbefalinger om standardene ISO 27001 og ISO 27002.* Oslo: Direktoratet for forvaltning og IKT.

Ekspertgruppen for forsvaret av Norge. (2015). *Et felles løft.* Oslo: Forsvarsdepartementet.

Frost, & Sullivan. (2017). *Global Information Security Workforce Study.*

Holmøy, E., Kjelvik, J., & Strøm, B. (2014). *Behovet for arbeidskraft i helse- og omsorgssektoren fremover.* Oslo–Kongsvinger: Statistisk sentralbyrå.

Højbjerre Brauer Schultz. (2017). *Efterspørgslen efter IT-sikkerhedsmedarbejdere i Hovedstadsområdet.* København: Højbjerre Brauer Schultz.

IKT-Norge. (2015). *Kritisk mangel på IKT-kompetanse .* Oslo: IKT-Norge.

Information Security Community on Linkedin. (2016). *Cloud Security Spotlight Report.* Crowd Research Partners.

Justis- og beredskapsdepartementet, Regjeringen Solberg. (2016). *Meld. St. 10. Risiko i et trygt samfunn — Samfunnssikkerhet.* Oslo: Justis- og beredskapsdepartementet.

Justis- og beredskapsdepartementet, Regjeringen Solberg. (2017). *Meld. St. 38 IKT-sikkerhet.* Oslo: Justis- og Beredskapsdepartementet.

Lysne-utvalget. (2015). *NOU 2015:13 Digital sårbarhet - sikkert samfunn.* Oslo: Justis- og beredskapsdepartementet.

Maurseth, P.-B., Holmen, R. B., & Løge, T. H. (2015). *Den norske IKT-næringens verdiskapingsbidrag.* Oslo: Menon Business Economics.

Norsis - Norsk senter for informasjonssikring. (2017). *Nordmenn og digital sikkerhetskultur.* Gjørvik: NORSIS.

Politidirektoratet. (2017). *Trusler og utfordringer innen IKT-kriminalitet.* Oslo: Politidirektoratet.

PriceWaterhouseCoopers. (2016). *Adjusting the Lens on Economic Crime - Preparation brings opportunity back into focus (Global Economic Crime Survey 2016).* PriceWaterhouseCoopers.

PriceWaterhouseCoopers. (2017). *Cyber Crime Survey 2017 - Norge og cybersikkerhet: Ledelsen har våknet, men evner de å holde tritt på utviklingen?* PriceWaterhouseCoopers.

Tømte, C., Olsen, D. S., Waagene, E., Solberg, E., Børing, P., & Borlaug, S. B. (2015). *Kartlegging av etter- og videreutdanningstilbud i Norge.* Oslo: Nordisk institutt for studier av innovasjon, forskning og utdanning.

Uninett AS. (2017). *Informasjonssikkerhet - IKT-strategi for norsk universitets- og høgskolesektor.* Oslo: KDs arbeidsgruppe for IKT-strategi og helhetlige løsninger.

van Lakerveld, J. A., Broek, S. D., Buiskool, B. J., Grijpstra, D. H., Gussen, I., Tönis, I. C., & Zonneveld, C. A. (2014). *Arbeidsmarkt voor Cyber Security Professionals.* Leiden: PLATO, University Leiden.

Wilson, B. A., Andrew, L., & Shaghil, A. (2004). Recent U.S. Macroeconomic Stability: Good Policies, Good Practices, or Good Luck? *Review of Economics and Statistics*, 824-832.

Tabelloversikt

Figuroversikt

Nordisk institutt for studier av
innovasjon, forskning og utdanning

Nordic Instititute for Studies in
Innovation, Research and Education

www.nifu.no