IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud

Michael Spjelkavik Mark
Cathrine Tømte
Terje Næss
Trude Røsdal

Arbeidsnotat 2017:8

NIFU

IKT-sikkerhetskompetanse i arbeidslivet – behov og tilbud

Michael Spjelkavik Mark
Cathrine Tømte
Terje Næss
Trude Røsdal

Arbeidsnotat 2017:8

Arbeidsnotat 2017:8

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

Prosjektnr. 12820757

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

Foto Shutterstock

ISBN 978-82-327-0282-4
ISSN 1894-8200 (online)

www.nifu.no

Forord

Dette notatet presenterer en kvantitativ studie av fremtidig tilbud på og etterspørsel etter IKT-sikkerhetskompetanse basert på framskrivningsmodeller utarbeidet av SSB. Oppdragsgiver har vært Justis- og beredskapsdepartementet, og oppdraget skal betraktes som et ledd i å opparbeide et solid kunnskapsgrunnlag for fremtidig tilbud på 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.

Oslo, juni 2017

Sveinung Skule
Direktør

Nicoline Frølich
Forskningsleder

Innhold

Sammendrag

IKT-sikkerhet ses på som en sentral utfordring på alle samfunnsnivåer; både 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, sett i forhold til arbeidslivets framtidige behov for slik kompetanse (både offentlig og privat sektor). Vår studie er metodisk basert på en kvantitativ framskrivning basert på forskjellige datakilder; MOSART, MODAG, registerdata og opplysninger om opptak og gjennomføring fra NSDs Database for statistikk om høgre utdanning (DBH).

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 betyr det at tilbudssiden må økes med vel en tredjedel, nærmere 37 prosent. Dette er ikke enkelt og vil kreve politisk handling.

Det er viktig å understreke at dette er framskrivninger og må tas med forbehold. Framskrivningene baserer seg på tilgjengelig informasjon og statistikk og bygger derfor i høy grad på historiske forhold. Vi har forsøkt å ta med den observerte økningen i antall studenter og uteksaminerte kandidater i årene 2012–2016. Men likevel ser vi en betydelig underdekning i år 2030.

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, MODAG for etterspørselsframskrivingene og mikrosimuleringsmodellen MOSART for tilbudsframskrivingene. 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, noe som gir en relativt sett liten populasjon. En mindre populasjon er mer sensitiv overfor plutselige endringer. Det kan for eksempel forekomme endringer i antall studenter eller markante endringer i etterspørsel som følge av et endret trusselbilde. En mindre populasjon vil altså øke usikkerheten ved framskrivninger.

IKT-sikkerhet står høyt på agendaen. Det er et viktig satsingsområde for regjeringen, og IKT-sikkerhet omfatter alle sektorer og henger sammen med regjeringens øvrige arbeid med samfunnssikkerhet. I tillegg inngår den foreliggende studien som en del av arbeidet med en nasjonal kompetansestrategi for IKT-sikkerhet. Dette arbeidet ble besluttet iverksatt i forbindelse med Samfunnssikkerhetsmeldingen (Meld. St. 10 (2016-2017)).

Begrepet IKT-sikkerhet

Begrepet IKT-sikkerhet defineres vanligvis som evnen til å forebygge, oppdage og håndtere tre typer hendelser. UNINETT[1] 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 imøtekomme 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 foreslo en kompetansestrategi for å styrke både utdanning og forskning på dette fagområdet.

Innenfor UH-sektoren 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, ved Universitetet i Bergen, ved Høgskolen i Oslo og Akershus og i et samarbeide 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 ligger på rundt 8–11 prosent av alle som tar utdanning som inneholder som 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

Den betydelige veksten i studenter og uteksaminerte kandidater til tross, 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 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.

[1] (UNINETT, s 7 (2017))

1 IKT-sikkerhet høyt på agendaen

Målet med foreliggende studie er å utvikle en forskningsbasert tilnærming som skal 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 og omfatter alle sektorer og flere nivåer. I tillegg må IKT-sikkerhet ses i sammenheng med regjeringens øvrige arbeid med samfunnssikkerhet. Slik vil foreliggende studie, som ser på tilbud på og etterspørsel etter IKT-sikkerhetskompetanse i lys av arbeidslivet, inngå som en del av regjeringens omfattende arbeid knyttet til områder med IKT-sikkerhet og samfunnssikkerhet som sådanne. 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 (2016-2017).

1.1 Begrepet IKT-sikkerhet

Før vi beskriver eget oppdrag 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 forståelsen 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. Og ikke nok med det, 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).

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).

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).

Tidligere i år kritiserte media myndighetenes håndtering av sensitive data, da det ble kjent at landets nødnett driftes av et selskap plassert i India (nrk.no). 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). 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» (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).

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.

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 i 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).

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).

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 imøtekomme 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, se Department for Business Innovation and Skills (2014)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. »*

Et nylig igangsatt 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, (PwC Cyber Crime Survey (2017)). Dette sammenfaller formentlig med at cyberkriminalitet blir sett på som en økende utfordring. I tillegg viser Cyber Crime Survey (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 imøtekomme 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. Og om kandidatene oppnår den kompetansen som etterspørres.

2 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. 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. Den andre typen består av IKT-sikkerhetsfag som tilbys på kurs som valgfritt eller enkeltfag. I dette avsnittet vil vi også gi en kort beskrivelse av utvalgte utdanninger og hvordan IKT-sikkerhetsutdanningene er sammensatt.

2.1 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.

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

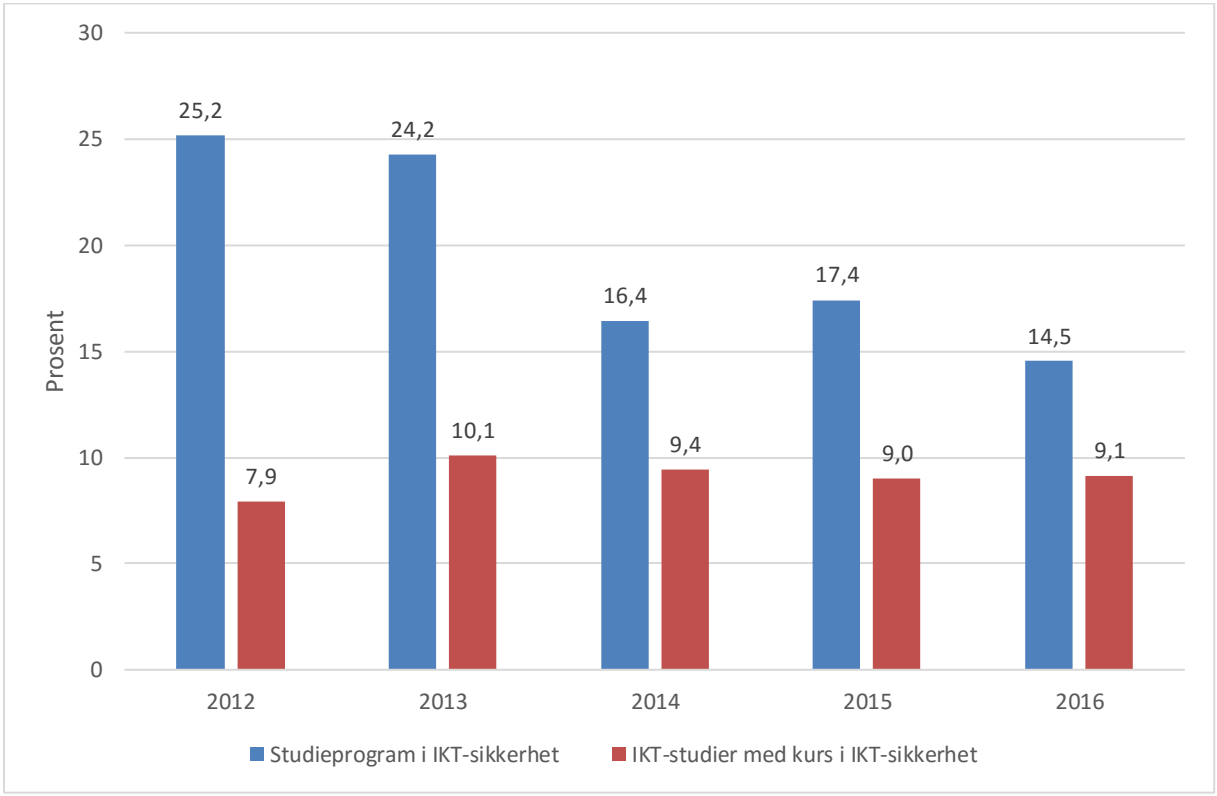
1) Inkludert Høgskolen i Sør-Trøndelag og Høgskolen i Gjøvik før 2016
2) Inkludert Høgskolen i Narvik før 2016
3) Inkludert Høgskolen i Nesna før 2016
4) Inkludert Norges Informasjonsteknologiske Høgskole før 2014
5) Inkludert Høgskolen i Vestfold før 2014

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

2.2 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.

2.2.1 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 informasjons-sikkerhet	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, risikohånd-tering 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 NTNU sine 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.

2.2.2 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

3 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..

3.1 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[2] har vi søkt å sammenfatte en mulig oversikt over IKT-sikkerhetsnæringen. Vår sammenstilling klarer å identifisere foretak som helt eller delvis opererer

[2] 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

3.2 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[3]. 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.

3.3 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[4].

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

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

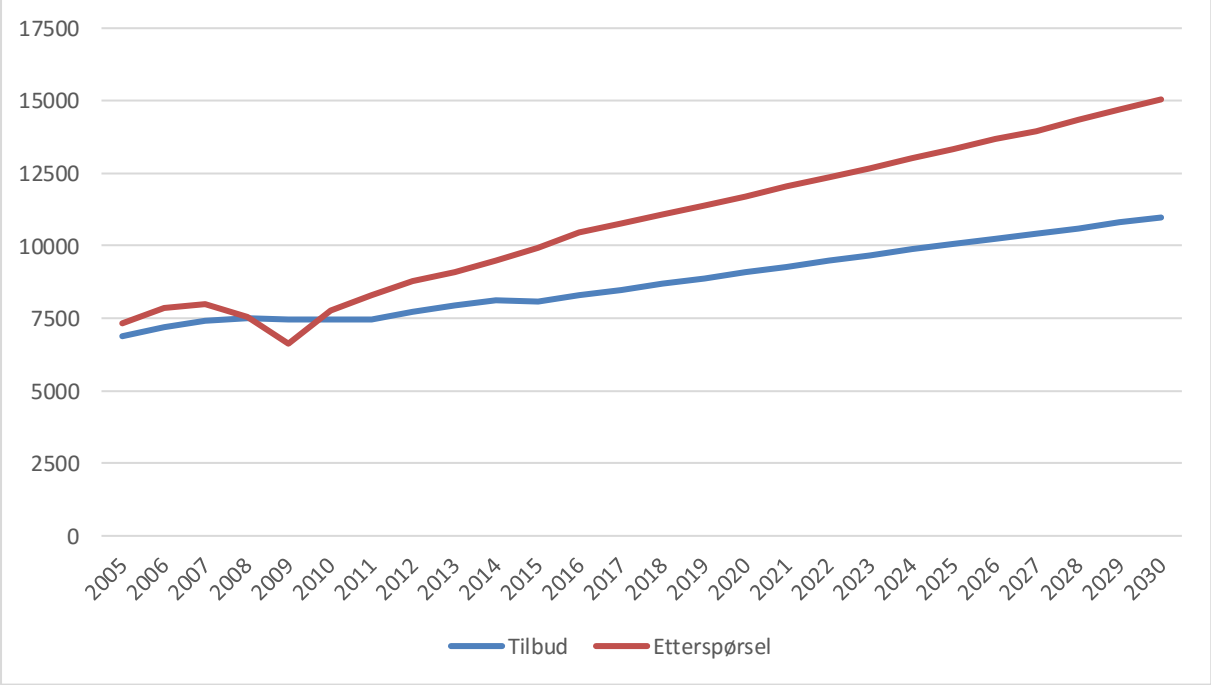
usikkert om disse utdanningene gir kandidatene den ønskede og etterspurte kompetansen. Vi har derfor valgt å nedjustere tilbudssiden fremfor å oppjustere etterspørselssiden.

- 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 imøtekomme 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[5]:

- 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.

3.4 Oppsummerende betraktninger

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

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

spørsmål er da om antall kandidater øker nok til å imøtekomme 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[6]. 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 arbeidskraftsinnvandring. 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.

[6] 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.

Vedlegg

Appendiks: Metode

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[7] 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

[7] 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.

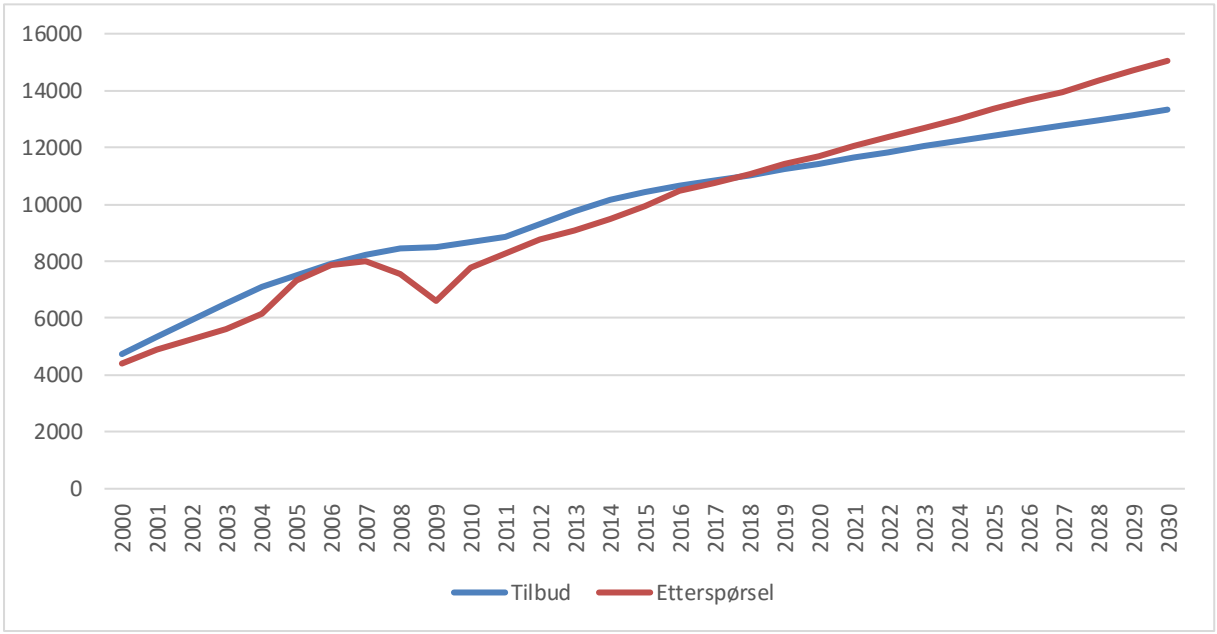
Appendiks: Basisframskrivning

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 3 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 3 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 3: Basisscenario tilbud og etterspørsel etter personell med IKT-sikkerhetskompetanse



Kilde: NIFU 2017

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, & Samfunnsøkonomiskanalyse. (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.

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.

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

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

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.

Meld. St. 10. (2016-2017). *Risiko i et trygt samfunn - Samfunnssikkerhet.* Oslo: Det Kongelige Justis- og Beredskapsdepartement.

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.

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

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