Uddannelses- og Forskningsministeriet

Prækvalifikation af videregående uddannelser - Intelligence og cyber studier

Udskrevet 13. november 2026

Master - Intelligence og cyber studier - Syddansk Universitet

Institutionsnavn: Syddansk Universitet
Indsendt: 29/01-2021 12:49
Ansøgningsrunde: 2021-1
Status på ansøgning: Godkendt
Afgørelsesbilag
Download den samlede ansøgning
Læs hele ansøgningen

Ansøgningstype

Ny uddannelse

Udbudssted

Syddansk Universitet, Campus Odense

Informationer på kontaktperson for ansøgningen (navn, email og telefonnummer)

Professor Trine Flockhart, Institut for Statskundskab, flockhart@sam.sdu.dk, +4565509261 Chefkonsulent Morten Vestergaard-Lund, movl@sam.sdu.dk, +4565501518 Afdelingsleder for HD- og Mastersekretariatet Britta Løck Worm, blwo@sam.sdu.dk, +4565504572 Vikki Michelle Thygesen, vmt@sdu.dk, +4565507105

Er institutionen institutionsakkrediteret?

Ja

Er der tidligere søgt om godkendelse af uddannelsen eller udbuddet?

Nej

Uddannelsestype

Master

Uddannelsens fagbetegnelse på dansk

Intelligence og cyber studier

Uddannelsens fagbetegnelse på engelsk

Intelligence and Cyber Studies

Angiv den officielle danske titel, som institutionen forventer at bruge til den nye uddannelse

Master i intelligence og cyber studier

Angiv den officielle engelske titel, som institutionen forventer at bruge til den nye uddannelse

Master of Intelligence and Cyber Studies

Hvilket hovedområde hører uddannelsen under?

Samfundsvidenskab

Hvilke adgangskrav gælder til uddannelsen?

Ansøgere til MICS skal have gennemført en relevant uddannelse indenfor det samfundsvidenskabelige, naturvidenskabelige eller humanistiske felt på enten professionsbachelor-, bachelor- eller kandidatniveau. Nedenstående er eksempler på videregående uddannelser, der giver adgang til optagelse på MICS, under forudsætning af relevant erhvervserfaring:

Professionsbacheloruddannelse indenfor offentlig administration, IT, diplomingeniør, kommunikation, sikkerhed, strategi og økonomi

Bachelor eller kandidatuddannelse indenfor statskundskab, jura, psykologi, sprog, økonomi, fysik, matematik, datalogi og softwareudvikling

For ansatte i Forsvaret er kravet at være officer under Forsvarsministeriets myndighedsområde – herunder også Beredskabsstyrelsen – på M321/U321 eller M322/U322 niveau.

Ansøgere til MICS skal som minimum have to års relevant erhvervserfaring efter at have gennemført den adgangsgivende uddannelse. Relevant erhvervserfaring kan udgøres af, at ansøgeren enten tidligere eller for nuværende beskæftiger sig med analyse, ledelse, efterretninger, informationssikkerhed, risikohåndtering, forsyningssikkerhed, forretningsudvikling og formidlingsaktiviteter.

Der kan søges om dispensation for ansøgere, der opfylder kravet om minimum to års relevant erhvervserfaring, men ikke opfylder uddannelseskravet.

Ansøgere skal have tilstrækkelige færdigheder i engelsk til at følge og forstå faglitteratur på engelsk og følge engelsksproget undervisning.

Ansøgere med udenlandsk eksamen skal endvidere have bestået Studieprøven i dansk som andetsprog. Det er et krav, at alle Studieprøvens 4 delelementer er bestået med karakteren 6 eller derover på 13-skalaen eller 02 på 7-trinsskalaen.

Studerende, der ikke ønsker at deltage i alle studiets elementer, kan optages som enkeltfagsstuderende, hvis forudsætningerne i henhold til adgang (se ovenfor) er opfyldte; hvis adgangskravene til det pågældende enkeltfag er opfyldt af den studerende, og hvis universitetet finder optagelsen hensigtsmæssig ud fra praktiske og pædagogiske hensyn. Grundfag I, From Cold War Espionage to Cyberwars: history, theory, and practice of intelligence and cybersecurity er obligatorisk for alle studerende. På grund af den faglige progression forventes den enkeltfagsstuderende at have tilegnet sig de samme faglige forudsætninger som den almindelige studerende. Der udstedes bevis for beståede fag og der kan udstedes et Certifikatbevis for den studerende der har gennemført mindst 30 ECTS og har skrevet et bestået Certifikatprojekt (5ECTS), altså i alt 35 ECTS.

Er det et internationalt samarbejde, herunder Erasmus, fællesuddannelse el. lign.?

Nej

Hvis ja, hvilket samarbejde?

Hvilket sprog udbydes uddannelsen på?

Dansk

Er uddannelsen primært baseret på e-læring?

Nej, undervisningen foregår slet ikke eller i mindre grad på nettet.

ECTS-omfang

60

Beskrivelse af uddannelsens formål og erhvervssigte. Beskrivelsen må maks. fylde 1200 anslag

Formålet med den nye masteruddannelse er at tilbyde en fleksibel og tilpasningsdygtig uddannelse på masterniveau, der løbende matcher kompetencebehovet inden for de to hastigt udviklende områder - intelligence og cyber. Uddannelsen vil øge deltagernes praktiske, analytiske og kritisk refleksive kompetence med et øje for at integrere deres eksisterende faglige specialisering inden for cyber og/eller intelligence.

Uddannelsen har til formål at tilbyde analytisk og kritisk refleksiv fordybelse i egen faglige specialisering ved at placere intelligence og cyber-relaterede spørgsmål i en bred kontekst af de udfordringer der følger i kølvandet på accelererende forandring, globalisering og digitalisering samt at udvikle deltagernes forståelse af de mange politiske, juridiske og etiske problematikker forbundet hermed. Uddannelsen har til formål at bidrage til løsningen af tværgående organisatoriske problemstillinger, sikre strategisk og informeret udsyn i både driftsmæssige og kritiske beslutningssituationer samt forståelse af de bredere samfundsmæssige konsekvenser forbundet med et nyt komplekst trusselsmiljø.

Uddannelses struktur og konstituerende faglige elementer

Uddannelsens kompetenceprofil:

Masteruddannelsen i intelligence og cyber studier (MICS) er rettet mod beslutningstagere, analytikere og specialister inden for myndighedsvæsnet, militæret, civilsamfundet og det private erhvervsliv. MICS er specielt rettet mod dem der ikke har en teknisk eller data-analytisk baggrund, men som ønsker at arbejde med sikkerhedsrelaterede spørgsmål inden for intelligence og/eller cyber områderne. Uddannelsen er et tilbud for personer, som ønsker at opkvalificere sig som led i fortsat karrieremæssig progression med sigte mod at opbygge viden om emner der i høj grad vil komme til at præge fremtidige arbejdsgange, strategisk planlægning og beslutningstagning. Tilbuddet kan også benyttes af personer, som ønsker en opdatering af forhold, som ikke har været en del af de pågældendes grunduddannelse inden for f.eks. statskundskab, tekniske uddannelser eller humaniora. Kompetenceprofilen afhænger af om specialisering ønskes og i så fald, hvilken specialisering deltageren vælger.

Viden

En master i intelligence og cyber studier giver de studerende viden om de mange udfordringer inden for intelligence og cyber områderne der er opstået i kølvandet på accelererende forandring, globalisering og digitalisering samt viden om de politiske, juridiske og etiske problematikker forbundet hermed. Undervisningen på MICS leveres i samarbejde mellem SDU og Forsvarsakademiet og hviler på den højeste internationale forskning og på praktisk og policy orienteret ekspertise. Centrale fagområder er: statens rolle og sårbarhed inden for intelligence og cyber; resilience og risiko; ansvar, lovlighed og etik inden for cyber og intelligence; foresight analysis, individuel og kollektiv data-analyse; teknologiske udfordringer og muligheder som f.eks AI; informationssikkerhed med mere. Til støtte for de centrale fagområder, har dimittenden desuden viden om nye fremtids- og scenariobaserede metoder og analyserammer for strategisk planlægning i et fundamentalt forandret trusselsmiljø og pågående transformative forandringer.

Færdigheder

En master i intelligence og cyber studier giver den studerende færdigheder i at styre og udvikle arbejdssituationer relateret til risikovurderinger, data-analyse og scenario-konstruktion under komplekse og usikre forhold. De studerende vil få færdigheder i at anvende nye løsningsmodeller og selvstændigt igangsætte og gennemføre fagligt og tværfagligt samarbejde og påtage sig professionelt ansvar.

De studerende vil kunne forstå, og på et videnskabeligt grundlag, reflektere over den tilegnede viden samt identificere relevante videnskabelige problemstillinger inden for fagområdet.

Kompetencer

Den masterstuderende kan, på basis af analyser, gennemført ved anvendelse af ovennævnte metoder, vurdere teoretiske og praktiske problemstillinger samt opstille nye analyse- og løsningsmodeller inden for intelligence og cyber områderne.

Den studerende kan derudover formidle faglige problemstillinger og diskutere fagrelevante problemstillinger med de relevante aktører inden for intelligence og cyber feltet.

En master i intelligence og cyber studier gør den studerende i stand til at tage ansvar for egen faglig udvikling.

Uddannelsens struktur

Uddannelsen udbydes af SDU i samarbejde med Forsvarsakademiet. Undervisningen er fordelt mellem de to institutioner med henblik på at drage størst mulig fordel af de to institutioners forskellige kernekompetencer. Master i intelligence og cyber studier er en tværdisciplinær uddannelse, som giver de studerende viden, færdigheder og kompetencer inden for fagområderne intelligence og cyber studier med afsæt i såvel teoretisk som empirisk viden. Uddannelsen styrker de studerendes evner til at analysere, komprimere og formidle efterretninger og cyberrelaterede spørgsmål.

Der er aftalt en specifik arbejdsfordeling mellem de to institutioner, hvor Forsvarsakademiet hovedsageligt vil løse undervisningsopgaver med et konkret fagligt indhold i forhold til intelligence og cyber, og SDU vil løse undervisningsopgaver af en mere teoretisk, begrebsmæssig og kontekstuel karakter i relation til de to fokusområder. Undervisningen vil for begge institutioners vedkommende være forskningsbaseret og leveret af fagligt højt kvalificerede undervisere.

Uddannelsen er opbygget efter et ”tragt-princip” hvor de studerende starter i det første semester med tre grundfag (hvoraf det første grundfag er obligatorisk for alle efterfølgende fag). De tre grundfag opbygger en bred viden om den historiske udvikling af såvel cyber- som efteretningsområdet og de mange udfordringerne og juridiske og etiske spørgsmål forbundet med både udførelsen, styringen og studiet af cybersikkerhed og efterretningsvirksomhed i et dynamisk og foranderligt sikkerhedsmiljø hvor målet er at sikre velfungerende og resiliente demokratiske samfund.

Uddannelsen består af følgende konstituerende faglige elementer:

3 grundfag (3 x 5 ECTS)
1 specialiseringsfag i enten intelligence eller cyber (10 ECTS)
2 workshopfag (foresight-analyse og simulering) (5 ECTS)
1 -3 valgfag med mulighed for yderligere specialisering (5 ECTS)
1 Master-projektforberedelsesfag (5 ECTS)
Et Master-projekt (15 ECTS)
Eventuelt efter fuldførelse af 30 ECTS - 1 Certifikat-projekt

Skematisk oversigt over uddannelsen

	Fag		
4. semester	**Masterprojekt** (15 ECTS)		
3. semester	**Valgfag** (5 ECTS)	**Workshopfag** (5 ECTS) Intelligence Analysis Simulation	**Projektforberedelsesfag** (5 ECTS) Obligatorisk masterprojektforberedelse eller Certifikat projektforløb
2. semester	**Specialiseringsfag** (10 ECTS) Cyber and Information Security eller Intelligence Analysis Eller 2 valgfag		**Workshopfag** (5 ECTS) Foresight analysis workshop
1. semester	**Grundfag I** (Obligatorisk) (5 ECTS) From Cold War Espionage to Cyberwars: history, theory, and practice of intelligence and cybersecurity	**Grundfag II** (5 ECTS) Governance and strategic decision-making in times of transformational change	**Grundfag III** (5 ECTS) Digital dilemmas of human data: Dependency, necessity, and privacy

Uddannelsen kan maksimalt forlænges til en total gennemførelsestid på fire år og kan afsluttes med et Certifikatprojekt (5 ECTS) efter at have fuldendt fag svarende til 30 ECTS (+ 5 ECTS for den afsluttende Certifikat opgave). Det anbefales, at man i størst mulig grad følger det foreslåede studieforløb for at få de fordele, der er, ved at følge en sammenhængende uddannelse med progression i undervisningen, hvor man som studerende følges som et hold og dermed bliver del af et vedvarende fagligt netværk.

Nedenfor følger en beskrivelse af mål og indhold af de planlagte konstituerende elementer af uddannelsen over de fire semestre.

Semester 1

På første semester følger fuldtidsstuderende tre grundfag. Semesteret starter med en introduktionsdag, hvor uddannelsen og de tre fag introduceres (3 semester studerende og studerende på enkeltfag vil også deltage i dette heldagsarrangement når uddannelsen er fuldt kørende). Dagen vil desuden byde på et fælles fagligt arrangement med gæsteforelæser, samt et socialt arrangement med netværksmuligheder. Derefter køres grundfag I i de første fem uger af semesteret, mens grundfagene II og III køres sideløbende i de sidste fem uger af semesteret.

From Cold War Espionage to Cyberwars: history, theory, and practice of intelligence and cybersecurity

Grundfag I - (5 ECTS) Obligatorisk

Fagets formål er at give et aktuelt og historisk indblik i hvilken rolle intelligence spiller i staten og statens rolle i styringen af ■■cyber-domænet. Fagets indhold fokuserer på kognitive, bureaukratiske, teknologiske, nationale og internationale sammenhænge inden for intelligence-styret beslutningstagning og cyberhåndtering. Faget er baseret på en bred vifte af faglitteratur fra forskellige tilgange til intelligence og cybersikkerhed inden for statskundskab, international politik, historie, strategiske studier, offentlige politikker og datalogi.

På cyber-området introduceres nøglebegreber inden for cybersikkerhed, statens sårbarheder overfor cyberangreb, mekanismerne for angreb, konsekvenserne for staten, og systemer til beskyttelse mod cyberangreb.

På intelligence-området introduceres nøglebegreber inden for intelligence såsom ”intelligence cyklussen”, intelligence indsamling, samt hvordan forskellige lande har divergerende intelligence kulturer, operationelle og institutionelle praksisser og strukturer.

Governance and strategic decision-making in times of transformational change

Grundfag II - (5 ECTS)

Faget sigter mod at give deltagerne en forståelse af det hurtigt skiftende og meget komplekse trusselmiljø, der i øjeblikket præsenterer adskillige udfordringer for styring og strategisk planlægning og beslutningstagning inden for efterretnings- og cyberfelterne. Faget introducerer de institutionelle styringsstrukturer inden for cyber og intelligence områderne og sigter mod at forbedre forståelsen af ■■begreber som ”risikosamfund” og ”resilience” som vigtige overvejelser i intelligence og cyberpraksis og styring. Faget vil omfatte nutidige udfordringer for strategisk planlægning og beslutningstagning såsom digitaliseringsprocessen i et komplekst miljø, hvor mange forskellige aktører spiller en rolle, enten som spoilere eller partnere. Faget vil omfatte et heldags seminar (sammen med grundfag III) om de særlige betingelser for småstater og for beslutningstagning og strategisk planlægning i en skandinavisk / dansk sammenhæng.

Digital dilemmas of human data: Dependency, necessity, and privacy

Grundfag III - (5 ECTS)

Dette fag undersøger de politiske, teknologiske, regulatoriske og etiske dilemmaer, der er involveret i arbejdet med systemer, der overfører, indsamler og bruger menneskelige data. Faget vil præsentere den studerende for eksempler på cases og nye trusler, der beder dem om at tilgå digitale dilemmaer fra en række forskellige analytiske tilgange. Den studerende bliver i forlængelse heraf udfordret til at reflektere over strategiske afhængigheder og værdier i deres egne organisationer. Fagets centrale temaer fanges af de globale rivaliseringer inden for informations- og kommunikationsteknologi såsom 5G og kunstig intelligens, statslige aktørers stræben efter digital autonomi og bekymringer om at bevare politisk suverænitet i omstridte partnerskaber med Big Tech. Udforskning af disse temaer vil ske gennem kritisk analyse af nødvendigheden af ■■overvågning versus individets ret til privatliv. Faget vil introducere deltagerne til vidtgående debatter omkring begreber som digital autoritarisme, udbyttende digitale teknologier, overvågningskapitalisme, våbengørelse af afhængigheder, afkobling af globale forsyningskæder, offensiv og defensiv brug af menneskelige data osv. Disse udfordringer tilgås fra et nordisk retsstatsperspektiv med liberale og demokratiske værdier, der skal navigere blandt små og store statslige aktører såvel som politiserede og sikkerhedsliggjorte globale relationer. Faget vil omfatte et heldagsseminar (sammen med grundfag II) om de særlige betingelser for småstater og for beslutningstagning og strategisk planlægning i en skandinavisk / dansk sammenhæng.

Semester 2

På andet semester følger de studerende enten et specialiseringsfag i cyber eller intelligence, eller de vælger to valgfag fra valgfags-kataloget. Semester 2/4 starter ligesom semester 1/3 med en introduktionsdag med introduktion af semesterets fag samt fælles faglige og sociale arrangementer. De to specialiseringsfag og valgfag udbydes sideløbende og efterfølges af et workshopfag med fysisk tilstedeværelse i slutningen af semesteret, hvori den opbyggede viden fra semester 1 & 2 afprøves i praksis.

Cyber and Information Security

Cyber- og informationssikkerhed

Specialiseringsfag - Cyber (10 ECTS)

Faget stiler efter at give de studerende forståelse af det tekniske fundament for cybersikkerhed og domænets historie, praksis og politiske debatter samt at introducere grundlæggende cybersikkerhedsværktøjer til identifikation og styring af netværkshændelser. Faget introducerer den studerende til computerens historie og styring af internettet, kryptografiens rolle og netværksmedicin, indtrængen og angreb. Disse principper anvendes til bredere diskussioner om begreber som tilskrivning, hændelsesrespons, risikostyring og resiliens og på forskellige trusselaktiviteter såsom kriminalitet, hacktivisme, desinformation, spionage og sabotage. Faget vil fokusere på udvalgte cyberrisikostyringsrammer og nationale cybersikkerhedsstrategier.

Intelligence Analysis

Efteretningsanalyse

Specialiseringsfag - Intelligence (10 ECTS)

Faget har til formål at give de studerende en forståelse af, hvordan usikkerhed kan vurderes og styres i efterretningsanalyse, og hvordan viden om nutidige driftsmiljøer og globale trusler kan oversættes til handlingsmæssig efterretning, der understøtter beslutningstagning. Faget sætter de studerende i stand til at vurdere, analysere og formidle en mangfoldighed af kilder og anvende kritisk tænkning, målcentrerede tilgange og almindelige grundlæggende strukturerede analytiske teknikker til at afbøde kognitiv bias og give overbevisende forståelse af komplekse intelligence-problemer. Desuden vil de studerende få forståelse for forskellige indsamlingsdiscipliner, såsom open source, human intelligence og aktivitetsbaseret intelligence, og deres grænser samt styrker og applikationer inden for forskellige efterretningsorganisationer. Med fokus på forholdet mellem nuværende intelligence praksis og langsigtede forudsigelser får de studerende anvendt forståelse af principperne og anvendelserne af foregribende analyse og estimerende metoder gennem scenariebaserede øvelser og trusselvurderinger.

Foresight analysis workshop

Workshop-fag I (5 ECTS)

Faget er en praktisk øvelse, der introducerer deltagerne til ”foresight analysis” (på dansk – fremsynsanalysetilgang) som et vigtigt element i strategisk beslutningstagning og politisk planlægning. Fremsyn er en fremadskuende tilgang, der har til formål at hjælpe beslutningstagere med at udforske og forestille sig hvad der kan ske i fremtiden. Der er ikke tale om at forsøge at forudsige fremtiden, men snarere at kunne forestille sig flere alternative ”fremtider” for at være bedre forberedt på de mange muligheder og udstyret til at påvirke og forme dem. Fremsyn involverer typisk systematisk fremtidig intelligensindsamling og mellemlang til lang sigt scenario-konstruktioner for at afdække megatendenser og opbygge en række mulige alternative scenarier for fremtiden. Fremsynsworkshoppen har til formål at give deltagerne viden om metoderne, værktøjerne og formaterne til strategisk fremsyn til at omformulere eksisterende opfattelser, tankesæt og begreber om fremtiden ved hjælp af metoden 'Multiple Scenario Generation'. Workshoppen vil gøre det muligt for beslutningstagere at tænke strategisk over fremtiden og reflektere over, hvordan de kan tilpasse sig til, og måske forme fremtiden. Workshoppen vil bruge et policyeksempel inden for cyberdomænet. Wokshoppen ledes i samarbejde mellem SDU og Hertie School of Governance og fordrer individuel forberedelse samt tilstedeværelse over et kort koncentreret forløb (3 dage).

Semester 3

På tredje semester har de studerende mulighed for yderligere specialisering gennem valg af et forskningsbaseret valgfag, gennem at anvende deres viden i en praktisk intelligence simulationsøvelse baseret på et cyber scenario, samt gennem at forberede deres Masterprojekt i et modul der gennemgår brug af teori, metode og forskningsdesign og giver deltagerne mulighed for at afprøve projektideer før et endeligt emne vælges.

Valgfagene vælges fra et katalog af valgfag der vil give den studerende mulighed for at tilpasse sin uddannelse yderligere til egne konkrete kompetencebehov. De valgfrie fag vil blive udviklet løbende og udbudt i efterårs- og forårssemesteret efter behov og vil altid afspejle aktuelle forskningsindsatser og konkrete arbejdssituationer på FAK og SDU. Enkeltfagsstuderende og studerende der ikke følger et specialiseringsfag, kan vælge flere valgfag der matcher deres behov. Deltagere kan vælge fra et løbende opdateret katalog af valgfag, som f.eks. kunne indeholde følgende moduler (flere valgfag forventes udviklet når rekruttering af nye kollegaer er på plads).

Intelligence Failures: From Pearl Harbour to Drone Warfare

Valgfag 1 (5 ECTS)

Fejl i intelligence operationer sker kontinuerligt, men det er kun sjældent at den brede offentlighed bliver opmærksom på sådanne fejlslagne intelligence operationer. Fejlslagne efterretningsoperationer er imidlertid særdeles vigtige for national sikkerhed, fordi de afslører ofte grundlæggende, mangler i et lands systemer for indsamling og analyse af data, rettidig beslutningstagning, undgåelse af bekræftelsesforstyrrelse, kritisk tænkning, effektiv advarselsfrihed og rollen som trusselindikatorer. Hvis den fejlslagne operation er højt profileret, kan den føre til øget politisk og offentlig kontrol af en normalt hemmelig efterretningsproces eller aktør. Vi behøver kun at tænke tilbage på de katastrofale begivenheder i Pearl Harbor eller 11. september for at se, hvordan efterretningsfejl har formet globale begivenheder og undermineret troværdigheden af ■■et efterretningsindsamlingsapparat. Faget vil analysere en række højt profilerede intelligence fejl for at forstå hvad der gik galt og hvad der kan forbedres i den nuværende efterretningsproces. Faget vil desuden inkludere analyse af sårbarheder og muligheder i efterretningsdeling mellem småstater og store stater, som for eksempel mellem Danmark og USA.

Warnings about War

Valgfag 2 (5 ECTS)

Hvad skal der til før advarsler om voldelig konflikt og krig bliver læst, troet og handlet efter? Hvorfor bemærkes nogle advarsler fra nogle kilder og accepteres stort set, mens andre ignoreres eller misbilliges? Dette fag søger at besvare disse spørgsmål gennem en tværfaglig tilgang, der kombinerer indsigt fra efterretningsstudier, fredsstudier og udenrigspolitisk analyse. Det udfordrer fremherskende antagelser, der har tendens til at bebrejde beslutningstagernes manglende modtagelighed og politiske vilje, og diskuterer, hvordan et lille antal faktorer former forskellige veje til succes eller fiasko. Faget fokuserer specifikt på de faktorer, der skaber den overbevisende virkning af konfliktadvarsler, der er formuleret fra udvalgte vestlige stater og IO'er, i modsætning til advarsler fra eksterne kilder såsom NGO'er eller nyhedsmedier. Faget inddrager specifikke eksempler på ”warning-response gaps” og inddrager praktikere, der er involveret i mekanismer til udvikling af advarselsrespons.

Cyber, Intelligence, and International Law

Valgfag 3 (5 ECTS)

I de senere år er cyberoperationer gentagne gange kommet frem i nyhederne og har demonstreret deres potentielle slagkraft og relevans for den bredere offentlighed: Atomfaciliteter er blevet saboteret; regeringswebsteder hacket, og det amerikanske præsidentvalg i 2016 blev udsat for massiv indblanding fra Rusland. Derudover er hadefuld tale og falske nyhedskampagner blevet et udbredt problem på sociale medier med store konsekvenser for demokratiets virke og legitimitet. Spørgsmålet der bliver stillet i dette fag er, om folkeretten har en rolle at spille i sådanne scenarier? Hvordan finder folkeretlige begreber som suverænitet eller jurisdiktion anvendelse på cyber området både i forhold til statslige og ikke-statslige aktører? Dette fag vil præsentere den eksisterende folkeretlige ramme for cyber- og efterretningsområderne og pege på huller, kontroverser, nye udviklinger og ikke mindst løsninger. Faget bruger casestudier og konfronterer deltagerne med spørgsmålet om, hvad der er lovligt og hvad der ikke er lovligt og legitimt.

Cyber Operations and Cyber War

Valgfag 4 (5 ECTS)

Dette fag bygger på specialiseringsfag ”Cyber ■■og informationssikkerhed” ved at tilføje geopolitiske og internationale sikkerhedsdimensioner. Faget undersøger en række dilemmaer for strategiske beslutningstagere i konkrete situationer. Dette inkluderer diskussion om afskrækkelse, tvang og eskaleringsrisici i cyberspace, bevarelse eller afsløring af softwaresårbarheder, integration af cybereffekter i militære operationer og koalitioner og fremme af ansvarlige internationale normer i cyberspace. Faget vil være scenariebaseret og omfatte forskellige bordopgaver og politiske forhandlingsspil. I løbet af faget vil den studerende tilegne sig færdighederne til at analysere og afveje forskellige strategiske muligheder inden for en række konkrete eksempler på cyber operationer.

Simulation Intelligence Analysis Exercise

Workshop-fag 2 (5 ECTS)

Simulation Intelligence Exercise udgør den anden praktisk øvelse på MICS-uddannelsen. Øvelsen giver deltagerne mulighed for at få praktisk erfaring med simulationers færdigheder og teknikker i intelligensindsamling og analyse. Faget vil give en praktisk og begrebsmæssig forståelse af styrkerne og faldgruberne ved kollektiv intelligenceanalyse, vurdering og beslutningstagning og vil give indsigt i de sandsynlige udfordringer, der er forbundet med at generere en aftalt kollektiv intelligence-vurdering af et relevant cyberscenarie. Workshoppen fordrer fysisk tilstedeværelse i en kort koncentreret forløb baseret på forudgående forberedelse.

Master-projekt forberedelse

Obligatorisk forberedelsesfag(5 ECTS)

Faget er specielt designet for studerende der har været uden for uddannelsessystemet for at forberede deltagerne på deres selvstændige Master-projekt. Faget skal sikre et positivt forløb i udfærdigelsen af det individuelle Master-projekt, og at Master-projektet lever op til de akademiske forventninger for et speciale på master niveau. Erfaring viser at grundig forberedelse før det selvstændige projekt påbegyndes giver et bedre resultat og en langt mere positiv oplevelse for den studerende. Modulet vil give de studerende indsigt i metode, anvendelse af teori og forskningsdesign, samt give dem mulighed for fremlæggelse og diskussion af ideer.

Certifikat-projekt

Frivilligt projekt forløb med individuel vejledning (5 ECTS)

Certifikat-projektet er en individuel opgave med vejledning i et relevant emne for masteren med inddragelse af refleksioner på de elementer den studerende har deltaget i. Certifikatprojektet er et tilbud til deltagere der har taget enkeltfag der tilsammen udgør mindst 30 ECTS men som ikke ønsker at gå videre med Master-projektet, eller til studerende som vælger ikke at fortsætte med hele masteren. Formålet med certifikat-projektet er dels at give deltageren mulighed for at reflektere over det valgte forløb og dels at give mulighed for at modtage et Certifikat-bevis som dokumentation for deltagelse af hvad der udgør ca. en ”halv master”.

Semester 4

I det fjerde og sidste semester arbejder studerende selvstændigt med det afsluttende master-projekt. Fjerde semester studerende starter semesteret sammen ved deltagelse i semesteret introduktionsdag og dennes faglige og sociale arrangementer.

Master-projekt

Individuel opgave med personlig vejledning (15 ECTS)

Masterprojektet er en substantiel individuel opgave, som skal dokumentere færdigheder i at anvende videnskabelige teorier og metoder under arbejdet med et fagligt afgrænset emne. Formålet med masterprojektet er, at den studerende udvikler sin viden, færdigheder og kompetencer til selvstændigt at indkredse og afgrænse en problemstilling, der har relevans for og relation til enten cyber- eller intelligence området for derefter selvstændigt at kunne gennemføre en empirisk og teoretisk undersøgelse af den valgte problemstilling. Der vil være mulighed for at skrive et erhvervsbaseret Master-projekt i samarbejde med deltagerens arbejdsplads, forudsat at specialet dokumentere færdigheder i at anvende videnskabelige teorier og metoder.

Begrundet forslag til takstindplacering af uddannelsen

Som en masteruddannelse med afsæt i det samfundsvidenskabelige hovedområde ønskes uddannelsen indplaceret under deltidstakst 1

Forslag til censorkorps

Uddannelsen ønskes primært tilknyttet censorkorpset for Statskundskab og sekundært Forsvarsakademiets Censorkorps for Forsvarets akkrediterede uddannelser. Videre er det et væsentligt perspektiv, at der grundet uddannelsens særlige genstandsfelter i nogen tilfælde vil være brug for en meget specialiseret viden fra censor, ligesom der i nogle tilfælde vil være brug for en censor med sikkerhedsgodkendelse.

Dokumentation af efterspørgsel på uddannelsesprofil - Upload PDF-fil på max 30 sider. Der kan kun uploades én fil

Master i intelligence og cyberstudier - behovsundersøgelse.pdf

Kort redegørelse for det nationale og regionale behov for den nye uddannelse. Besvarelsen må maks. fylde 1800 anslag

Cybertruslen mod Danmark vurderes, som nævnt, af Center for Cybersikkerhed i 2020 som ”alvorlig”. Angreb og effekter finder sted i et komplekst rum af sociale dynamikker, der kræver en bredere samfundsvidenskabelig analyse og forståelse af cybersikkerhed for at se udover kun it-systemer og data. De økonomiske, politiske og sociale effekter af sådanne angreb understreger nødvendigheden af at opbygge modstandsdygtige/resilliente samfundsstrukturer parallelt med Danmarks accelererende digitale omstilling, men hidtil har løsninger primært været søgt i tekniske tiltag.

Denne tilgang har været reflekteret i uddannelsesudbuddet og samtidigt genererer dette udbud flere tekniske initiativer. MICS bryder med denne cirkel ved at forskubbe fokus til efterretningspraksisser og samfundsmæssige risikoanalyser, der lægger et nyt og nødvendigt lag ind i det resiliente samfunds kompetenceopbygning.

Under afsnittet for Kriterium 2 gennemgås beslægtede uddannelser til MICS og konkluderer, at der ikke findes et tilsvarende udbud med en kompetenceprofil, der adresserer de bredspektrede cybertrusler, som danske myndigheder, private virksomheder og samfundsbærende institutioner er underlagt. Ligeledes drives behovet frem af nationale politiske cybersikkerhedsinitiativer fra skiftende danske regeringer samt et lokalt organisationsdrevet momentum om business continuity, der udmønter sig i behovet for videre- og efteruddannelse på området.

Behovsanalysen peger på cybertrusler som grænseoverskridende og dermed ikke geografisk betinget. Dog er der en naturlig fortættet tilstedeværelse af store organisationer i hovedstadsområdet, der i højere grad end mindre organisationer vil have ressourcer og incitament til at benytte MICS-uddannelsen, hvilket også aflæses i surveyresultaterne.

Uddybende bemærkninger

Uddannelsen er et initiativ med afsæt i løbende dialog mellem de to uddannelsesinstitutioner om hvordan aktuelle uddannelsesbehov fra tre centrale myndigheder, Politiets Efterretningstjeneste, Forsvarets Efterretningstjeneste og Forsvaret, bedst vil kunne mødes. En forpligtende interesse fra disse myndigheder understreger efterspørgslen, da alle tre vurderes at være ”kritiske kunder”, der har udprægede forudsætninger for at vurdere behov og relevans. Myndighederne har tilkendegivet behov for op til 13-15 fuldtidsstuderende og 6-7 enkelt-modulstuderende. Denne anerkendelse sender et positivt signal til andre interessenter.

Disse konkrete behov drives af et generelt højnet trusselsniveau med deraf øget behov for MICS-kompetencer. Center for Cybersikkerhed (CfCS) under Forsvarets Efterretningstjeneste vurderer i trusselsvurderingen for 2020, at "Cybertruslen er en alvorlig trussel mod Danmark. Cyberangreb har især økonomiske og politiske konsekvenser." Det seneste forsvarsforlig 2018-2023 har i lyset af disse trusler afsat 1,5 mia. kroner til Danmarks digitale sikkerhed, der blandt andet udmøntes gennem 25 initiativer i "National Strategi for Cyber- og Informationssikkerhed 2018-2021". Derudover stiller både NATO og EU øgede krav om cybersikkerhed og -kapaciteter. Kommende lovgivning om investeringsscreening i de kritiske sektorer samt regeringens politireformudspil om en ny samlet national efterforskningsenhed peger sammen med stigende budgetter for FE og PET i retning af større cyber- og informationssikkerhedsbehov.

Med inspiration fra Cyber- og Informationssikkerhedsstrategiens udpegning af kritiske sektorer er der gennemført kvalitative interviews med 14 udvalgte sektor- og brancherepræsentanter – mange af dem på leder-niveau - for at afdække efterspørgsel og overlappende kompetencebehov.
Derudover er der gennemført en elektronisk survey-undersøgelse blandt 135 lignende respondenter i sektorspecifikke stillinger med en svarprocent på cirka 40% (54 respondenter). Resultatet af disse behovsundersøgelser viser behov og efterspørgsel på MICS på både nationalt og regionalt plan samt i de kritiske sektorer med et usikkert estimat på 2-5 fuldtidsstuderende og 6-10 enkeltmodulsstuderende.

Se venligst den detaljerede behovsanalyse for uddybende oplysninger.

Underbygget skøn over det nationale og regionale behov for dimittender. Besvarelsen må maks. fylde 1200 anslag

Der er et akut og stigende behov for kombinationen af efterretnings- og cybersikkerhedskompetencer i en bred vifte af danske private og offentlige sektorer og den kommende udgave af den Nationale strategi for cyber- og informationssikkerhed vil præsentere endnu flere MICS-relevante initiativer – eksempelvis større forankring af cybersikkerhed hos topledelser, hvilket kræver en organisation, der er gearet til dette samt større fokus på uddannelse inden for cybersikkerhed.

Vi har fra forsvars- og politimyndigheder tilkendegivelser om konkret årligt behov for op til 13-15 studerende per år på hele uddannelsen i de første tre år, og mindst 6-7 studerende på enkeltmoduler. Dertil kommer et foreløbigt estimat på 2-5 fuldtidsstuderende og 6-10 enkeltmodulsstuderende fra andre aktører baseret på behovsanalysens resultater. Forventningen er, at disse studerende vil fordele sig nogenlunde ligeligt mellem denne uddannelse og den ansøgte engelsksprogede udgave af uddannelsen.

Hvilke aftagere har været inddraget i behovsundersøgelsen? Besvarelsen må maks. fylde 1200 anslag

Behovsanalysen har fundet sted via to konsultationsspor: Spor 1, forsvars- og politimyndigheder, og spor 2, offentlig-privat sikkerhedsspor. Klassificering af oplysninger sætter grænser for afrapportering om spor 1, der er foregået på ledelsesniveau mellem FAK og efterretningstjenesterne og på baggrund af interne behovsanalyser. Både uformelle og formelle møder har sikret afstemning af konkrete behov for indholdet af de to specialiseringsfag i dialog med:

- Forsvarskommandoen

· Forsvarets Efterretningstjeneste

· Politiets Efterretningstjeneste

· Forsvarsministeriets Materiel- og Indkøbsstyrelse

Spor 2 har haft mulighed for at tilgå behovsafklaringen gennem en mere åben proces via 12 kvalitative interviews med 14 respondenter og 54 besvarelser fra den elektroniske survey. Respondenterne dækker qua deres centralt placerede stillinger (DCIS, CISO, internationale virksomheder, myndigheder, brancheforeninger osv.) et bredt udsnit af personer fra dansk cyber- og informationssikkerhed. Begge analyser har informeret og formet tilrettelæggelsen af MICS i forhold til de faglige og praktiske kompetencebehov, der efterspørges.

Hvordan er det konkret sikret, at den nye uddannelse matcher det påviste behov? Besvarelsen må maks. fylde 1200 anslag

Forsvarsministeriet har udpeget cyber-domænet som et indsatsområde, der vil vækste i både ministeriet, Forsvaret, FE og PET. Imidlertid eksisterer der ikke en uddannelse der har øje for den sikkerhedspolitiske kontekst samt har både et globalt og et skandinavisk perspektiv. Derfor er der et behov for en uddannelse der kæder disse elementer sammen.

Uddannelsesforslaget er udfærdiget gennem dialog med de myndigheder der eksplicit har bedt om en uddannelse af denne slags sammen med centralt placerede aktører i de offentlig-private cybersamarbejder. Ønsket hos myndighederne har været en uddannelse der forener den militær-specifikke tilgang, der kendetegner uddannelserne på FAK med den teoretiske og begrebsfunderede tilgang der kendetegner en universitetsuddannelse. Desuden er der et ønske blandt aftagerne om fleksibilitet og mulighed for at kunne tage enkelte relevante moduler uden forpligtelse til at gennemføre hele uddannelsen, prioriteret netværksdannelse, fokus på praksisnærhed og en organisatorisk oversætter-kompetence mellem det tekniske og det samfundsvidenskabelige. Uddannelsen er tilpasset og matcher disse ønsker (se uddybning i behovsanalysen).

Beskriv ligheder og forskelle til beslægtede uddannelser, herunder beskæftigelse og eventuel dimensionering. Besvarelsen må maks. fylde 1200 anslag

MICS bringer med sin særlige fagkombination og samfundsvidenskabelige tilgang en unik uddannelse og kompetenceprofil på markedet, der ikke bliver matchet af sammenlignelige udbud. MICS åbner for en ny type opkvalificering og nye stillingskategorier uden at forringe andre uddannelsers vilkår, da der ikke er noget uddannelsesmæssigt overlap. Samarbejdet mellem SDU og FAK udfylder et tomrum, som andre udbud tilnærmer sig fra en mere specialiseret og teknisk vinkel eller de henvender sig direkte til Forsvarets ansatte gennem enkeltstående fag.

De eksisterende (teknisk fokuserede) masteruddannelser i cybersikkerhed dækker ikke det efterretningsmæssige sigte for MICS, mens de eksisterende efterretningsudbud (enkeltstående fag i Forsvarets regi) ikke dækker det brede akademiske sigte for MICS. Den eventuelt mest sammenlignelige uddannelse er Københavns Universitets engelsksprogede kandidatoverbygning i Security and Risk Management (120 ECTS), der har visse overlap med MICS ved at opbygge risikoanalytiske kompetencer og udbyde faget Intelligence (7,5 ECTS). Det er dog ikke en master og udbyder ikke sammenlignelige praksisnære kompetencer, som FAKs særlige ekspertise er garant for.

Uddybende bemærkninger

Berøringsflader til andre uddannelser

Da der ikke findes nogen direkte beslægtede eller konkurrerende uddannelser til MICS i Danmark på hverken det professionelle master-niveau eller som fuldtidsstudieudbud, orienterer behovsanalysens sammenligning sig i stedet mod tilnærmende uddannelser ved at selektere på overlap med dele af MICS' faglige fokus. Der findes tre store berøringsflader til tilnærmende uddannelser, der i forskellig grad udgøres af henholdsvis 1) efterretningsanalyse og -ledelse, 2) governance/styring af de to domæner - cyber- og informationssikkerhed og 3) risikoanalyse- og strategisk planlægning og management. Graden af overlap med MICS er hovedsageligt betinget af uddannelsernes teknik- og efterretningssigte samt uddannelsesspecialisering. Resultatet er, at heller ingen af de tilnærmende uddannelser kan udgøre et alternativ til MICS. Se venligst behovsanalysen for en detaljeret sammenligning.

Beskriv rekrutteringsgrundlaget for ansøgte, herunder eventuelle konsekvenser for eksisterende beslægtede udbud. Besvarelsen må maks. fylde 800 anslag

Studerende på uddannelsen vil typisk være personer, der bestrider hverv inden for offentlige myndigheder og relevante virksomheder i den private sektor. Særligt forventes en andel af studerende med en baggrund som analytikere fra Forsvarets Efterretningstjeneste (FE), ansatte i efterretningsstillinger i forsvaret samt fra Politiets Efterretningstjeneste (PET). Endvidere antages det at en mindre andel af de studerende vil komme med en baggrund fra den private sektor, især "risk advisory companies".

Da uddannelsen udfylder et nyt behov og der ikke pt. findes lignende uddannelser, vil MICS ikke have konsekvenser for rekrutteringen til andre uddannelser. Det er dog muligt at uddannelsen vil konkurrere med videreuddannelsesudbud i den private sektor og internt i de relevante myndigheder.

Beskriv kort mulighederne for videreuddannelse

Muligheden for at tage enkelte moduler og muligheden for at opnå et Certifikat Bevis udgør en videreuddannelses mulighed inden for de overordnede rammer af MICS. Dette antages at ville være særligt relevant for personer hvis uddannelse ikke tog højde for cyber- og intelligence områderne på uddannelsestidspunktet.

Forventet optag på de første 3 år af uddannelsen. Besvarelsen må maks. fylde 200 anslag

20-30 pr. år, hvoraf der er forhåndstilkendegivelser på hovedparten, som ventes at fordele sig lige mellem denne og den ansøgte engelske udgave af uddannelsen. Se 'Øvrige bemærkninger til ansøgningen'

Hvis relevant: forventede praktikaftaler. Besvarelsen må maks. fylde 1200 anslag

Ikke relevant

Øvrige bemærkninger til ansøgningen

Tilkendegivelser fra FAK, PET, Forsvarsministeriet og FE indikerer –op til 13-15 fuldtidsindskrivninger om året de første tre år, samt 6-7 modulstuderende. Vi har en forsigtig forventning om ca. 10 andre studerende per år. Forventningen er, at disse studerende vil fordele sig nogenlunde ligeligt mellem denne uddannelse og den ansøgte engelsksprogede udgave af uddannelsen.

En mindre del af den dansksprogede uddannelse forventes gennemført på engelsk. En væsentlig årsag hertil er, at engelsk er det mest relevante fag- og forskningssprog inden for både intelligence og cyber, og at flere undervisere derfor ikke vil være dansktalende, ligesom intelligence og cyber som arbejdsdiscipliner i deres udgangspunkt er grænseoverskridende.

Ud fra ovenstående betragtninger og med baggrund i en vurdering af, at der foreligger betydelig interesse for en engelsksproget MICS-uddannelsen, vil samtidig prækvalifikation af en dansksproget og en engelsksproget version af uddannelsen dels ramme et eksisterende behov på arbejdsmarkedet, dels give en unik mulighed etablering af et overordnet læringsfællesskab hvor fag for de to versioner af uddannelsen sam-undervises og hvor deltagerne hver især indgår på deres egne præmisser i forhold til deres ønsker om fleksibilitet, specialisering, varighed og deres individuelle erhvervsorientering.

Vedrørende e-læring:

Uddannelsen tilrettelægges således, at store dele af undervisningen vil blive tilrettelagt som blended learning kombineret med online fag, der ikke, eller kun i begrænset omfang kræver fysisk tilstedeværelse.

Fysisk fremmøde vil indgå som et element i netværksdannelsen. Hvert semester vil starte med et heldagsarrangement, der vil inkludere både faglige og sociale elementer, så deltagere i uddannelsen får lejlighed til at netværke på tværs af fagog årgange. Ydermere vil nogle af uddannelsens faginkludere yderligere arrangementer med fremmøde (de 2 workshopfag), og i nogle tilfælde (Specialiseringsfag Intelligence Analysis) er der planlagt et internatophold. Datoer for undervisning med fysisk fremmøde og internat vil indgå i langtidsplanlægningen af uddannelsen, således at de studerende kan planlægge deres deltagelse.

Hermed erklæres, at ansøgning om prækvalifikation er godkendt af institutionens rektor

Ja

Status på ansøgningen

Godkendt

Ansøgningsrunde

2021-1

Afgørelsesbilag - Upload PDF-fil

A 5 -Afgørelsesbrev- Master i intelligence og cyber studier SDU.pdf

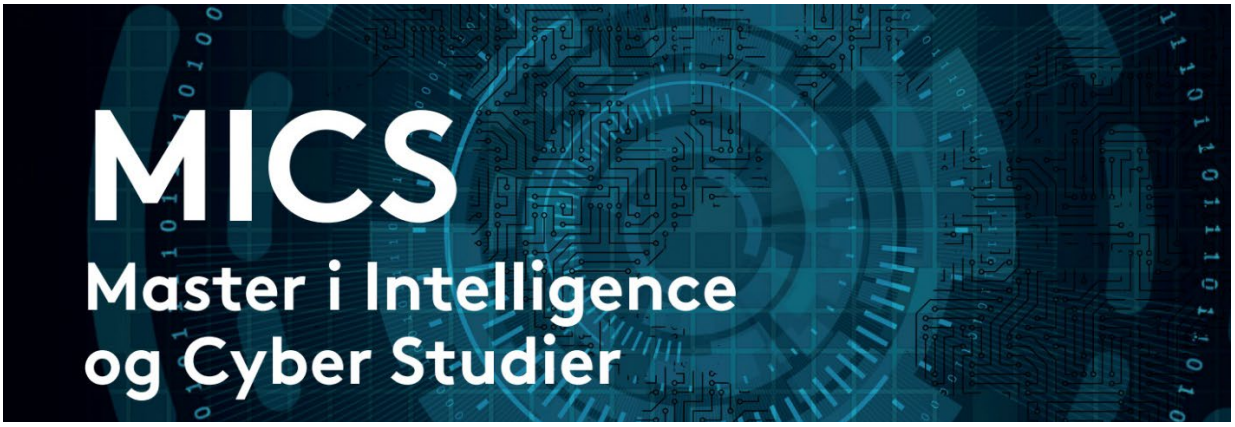
Samlet godkendelsesbrev - Upload PDF-fil

Master i intelligence og cyber studier

Bilag til prækvalifikationsansøgning den 1. februar 2021

Indhold

1. Behovsundersøgelse for Master i intelligence og cyber studier



Bilag 1

Behovsundersøgelse for Master i Intelligence og Cyber Studier

Indhold

1. Introduktion til MICS 3
2. Behovsanalysens formål og struktur 3
3. MICS og beslægtede uddannelser 4
3.1. Et unikt samarbejde mellem SDU og FAK 7
3.2. Berøringsflader til andre uddannelser 7
4. Baggrund for behovsanalysen 8
4.1. Et højnet trusselsniveau driver et øget behov for MICS-kompetencer 8
4.2. Efterspørgsel fra myndighedsområder i vækst 10
4.3. Civile samfundsaktørers behov for stærkere cyberkompetencer 11
5. Baggrunden for to separate behovsanalyser 11
6. Behovsanalyse spor 1: Behov for MICS-uddannelsen inden for forsvars- og politiområdet 12
6.1. Generelt behov for cyberuddannelser 12
6.2. Generelt behov for efterretningsuddannelser 12
6.3. Konkret behov for Master i Intelligence og Cyber Studier 13
7. Behovsanalyse spor 2: Behov for MICS-uddannelsen i det offentlig-private sikkerhedsspor 14
7.1. Behovsanalysens metode og respondenter: Kvalitative interviews 14
8. Behovsanalysens metode og respondenter: Elektronisk survey 15
9. Relevans af MICS og estimat over antal potentielle studerende 18
9.1. Nationalt og regionalt behov for MICS 19
9.2. Match mellem MICS og behovsanalysen: Fagligt indhold og uddannelsens tilrettelæggelse 20
10. Behov for sprogligt udbud af MICS på engelsk 24
11. Konklusion på behovsanalysen 26

1. Introduktion til MICS

Uddannelsen Master i Intelligence og Cyber Studier (MICS) bygger på et nyskabende samarbejde mellem Syddansk Universitet og Forsvarsakademiet, der gør den studerende i stand til at forstå, formidle og reagere på voksende og i stigende grad komplekse trusselsbilleder. MICS opbygger kompetencer indenfor cyber og intelligence med mulighed for specialisering og stor fleksibilitet. Uddannelsen giver adgang til Forsvarets praksisorienterede ekspertise i kombination med universitetets internationale faglige netværk og analytiske tilgang. Uddannelsen favner emnemæssigt bredt ved at undervise i metodiske, politiske, teknologiske, juridiske og økonomiske aspekter af de mange reelle trusler fra eksempelvis (industri)spionage, finansielt motiveret cyberkriminalitet, digital overvågning og dataindhentning.[1] MICS henvender sig således til personer, der arbejder med cyber- og informationssikkerhed i en myndighed eller industrien, skal navigere i udfordrende spændingsfelter mellem det politiske og teknologiske, skelne mellem potentielle partnere og ondsindede aktører og være på forkant med nye trusler. MICS er udviklet som et direkte svar på efterspørgsel fra Forsvarets Efterretningstjeneste (FE), Politiets Efterretningstjeneste (PET) og Forsvaret og er udtryk for det stigende behov for kompetencer indenfor intelligence og cyber-områderne.

Behovsanalysen har ført til en række tilpasninger af MICS-uddannelsen, hvilket også fremgår i det nedenstående. En central tilpasning angår uddannelsens sprog. Oprindeligt var MICS planlagt som en dansksproget professionel master med udgangspunkt i behov og undervisningstraditioner indenfor især Forsvaret, men behovsafdækningen i det bredere samfund har blotlagt, at der her både er et ønske og klart behov for at MICS også er tilgængelig for udenlandske medarbejdere. Dette har betydet en tilpasning af uddannelsen, der muliggør ansøgning om prækvalificering af både en dansk og engelsk version af MICS, der samundervises indenfor ét enkelt læringsfællesskab. Baggrunden skal findes i, at der blandt respondenterne blev udtrykt bekymringer over at en dansksproget MICS vil være utilgængelig for den voldsomt stigende andel af udenlandsk arbejdskraft i informations- og cybersikkerhedsbranchen. Arbejdskraftmangel på kvalificerede specialister er et globalt problem og i Danmark kommer det til udtryk gennem øget tilstrømning fra udlandet, men også i manglende håndtering af sårbarheder og sikkerhedsbrud. I lyset af respondenternes bekymringer har behovsanalysen efterfølgende undersøgt problemets omfang og fundet et absolut veldokumenteret behov. Udbuddet af en engelsk version af MICS er således født af en konkret, anerkendt og voksende problemstilling, der ikke alene kan hjælpe til at opfylde et stigende arbejdsmarkedsbehov, men som også bidrager til at højne Danmarks generelle cybersikkerhed. Der redegøres i detaljer for dette under afsnit *10. Behov for sprogligt udbud af MICS på engelsk*.

2. Behovsanalysens formål og struktur

Det er af afgørende betydning for udviklingen og udbuddet af MICS, at der kan konstateres et konkret behov for uddannelsens genstandsfelt og kompetenceprofil. Forudsætningen for dette konkrete match hviler på dialog med uddannelsens aftagere. Behovsanalysens formål er derfor at afdække uddannelsesmarkedets behov for MICS ved henholdsvis at undersøge beslægtede uddannelsesudbud og præsentere MICS for en række centrale aftagere inden for cyber- og informationssikkerhed.

[1] Kompleksiteten i trusler mod cyber- og informationssikkerhed stiger parallelt med at opmærksomheden på ikke-tekniske sårbarheder højnes. Insider-trusler, usikre forsyningskæder og hastigt forandrede forhold i globale politiske og økonomiske relationer stiller større krav til organisationers evne til at kombinere forskellige sikkerhedskompetencer. MICS-uddannelsen fokuserer på dette behov ved at kultivere kompetencer til at tænke strategisk på tværs af problemstillinger, organisationer og eksterne afhængigheder. Se fx Henry Farrell og Abraham L. Newman (2019): "Weaponized Interdependence: How Global Economic Networks Shape State Coercion", *International Security*: https://www.mitpressjournals.org/doi/abs/10.1162/isec_a_00351?journalCode=isec

Gennemførelsen af behovsanalysen har givet værdifuld information. Respondenterne har leveret både positiv feedback og konstruktiv kritik, der har resulteret i tilpasninger af uddannelsens indhold og udformning og de mange kontakter til aftagerne har sikret en særlig plads til både myndighedernes og virksomhedernes perspektiver. Det er denne proces, der har affødt udviklingen af både en dansk- og engelsksproget version af MICS. Disse aftagerperspektiver er især vigtige i udviklingen af MICS som en professionel master, der henvender sig til erhvervsaktive personer og som i høj grad afhænger af arbejdsgivernes opbakning. Behovsanalysen har således gennem formel og uformel dialog, kvalitative interviews og en elektronisk survey understøttet et større match med aftagernes behov.

Behovsanalysens struktur er som følger. Først bliver uddannelsesmarkedet afsøgt for udbud beslægtet med MICS. Det sker gennem en systematiseret sammenligning af fagligt indhold og det konstateres, at MICS har en unik uddannelsesprofil. Dernæst præsenteres en analyse af det aktuelle og forventede trusselsbillede hvilket anses for at være styrende for behovet for MICS-kompetencer. Et højnet trusselsniveau på cyber- og informationssikkerhedsområdet betyder en fortsat vækst hos især forsvars- og politimyndigheder med Forsvarets Efterretningstjeneste og Politiets Efterretningstjeneste i front. Det konstateres også, at politiske tiltag angående cybersikkerhed betyder højere og mere komplekse krav til cyberkompetencer hos civile aktører. Behovsanalysen går herefter i dybden med afdækningens resultater fra henholdsvis forsvars- og politiområdet (klassificeret analyse) og det offentlig-private sikkerhedsspor. De to analyser påviser konkrete behov for MICS hos FE, PET og Forsvaret, der tilkendegiver at sende op til 13-15 fuldtidsstuderende og 6-7 modulstuderende på MICS-uddannelsen. Der konstateres ligeledes behov for MICS-kompetencer i den private sektor og hos andre civile myndigheder. Indikationerne fra disse aftagere, der har deltaget i behovsanalysens, er at der er stor interesse for uddannelsen med en forsigtig forventning om 2-5 fuldtidsstuderende og 6-10 modulstuderende fra de adspurgte aftagere i uddannelsens første par år med en antaget efterfølgende stigning i takt med at kendskabet til uddannelsen øges og behovet stiger (jvf. afsnit 10). Endelig redegøres der for behovet for en engelsksproget version af MICS, hvilket understøttes af statistisk materiale over arbejdskraftsunderskud og øgning i antallet af udenlandske specialister. Behovsanalysens resultater viser således både efterspørgsel og tilgang til MICS.

3. MICS og beslægtede uddannelser

Dette afsnit præsenterer et overblik over hvilke beslægtede uddannelser, der allerede findes på det danske uddannelsesmarked. Behovsanalysens detaljerede resultater vil blive præsenteret efter afsøgningen af uddannelsesmarkedet, da det er passende først at klarlægge i hvilken grad MICS adskiller sig fra beslægtede uddannelser på markedet. Afsøgningen tager et bredt sigte og er systematiseret i nedenstående tabel. Det brede sigte er nødvendigt, da der ikke findes en lignende uddannelse på det danske marked.

Den nedenstående behovsanalyse viser både efterspørgsel og opbakning til uddannelsens særlige karakter og da der ikke findes et konkurrerende alternativ i Danmark, placerer det MICS på forkant med den nationale udvikling. Et eksempel på en lignende udenlandsk uddannelse er Intelligence and Security Studies, der udbydes som en 1-årig fuldtidsmaster eller som et 2-årigt deltidsstudie på det britiske Brunel University London. De positive erfaringer fra denne uddannelse er, at kandidaterne finder beskæftigelse i både det offentlige og private samt opnår karriereavancement på baggrund af masteren.[2] Cyber- og efterretningsudfordringerne kender ingen landegrænser og derfor står

[2] Brunel rapporterer følgende om kandidaters beskæftigelse: *"Kandidater sikrer sig job i den private og offentlige sektor, hvor de fleste forfølger karrierer inden for efterretnings- og sikkerhedsstudier. De, der allerede er i beskæftigelse i det offentlige, oplever at kurset hjælper med forfremmelse, at blive kommitteret eller giver nye beskæftigelsesmuligheder efter pensionering. Den private sektors muligheder er især stærke inden for analytiske funktioner i bank-, ressource- og risiko- og*

Storbritannien og Danmark overfor de samme trusselstyper og har lignende kompetencebehov. Beslægtede uddannelser til MICS har således fundet anvendelse i udlandet og bør derfor også kunne introduceres herhjemme.

Da en del af de samlede elementer på MICS i nogen grad genfindes i særskilte eksisterende uddannelsesudbud undersøges de potentielle overlap med uddannelser, der overordnet set er ret distanceret fra MICS. Derudover er en del af nedenstående kurser medtaget, fordi flere af respondenterne i behovsanalysens kvalitative interviews identificerede et vist slægtskab med MICS.

sikkerhedssektorerne." Brunel University London (2020): *Intelligence and Security Studies MA* https://www.brunel.ac.uk/study/postgraduate/intelligence-and-security-studies-ma

Sammenlignende uddannelsesoversigt*

Fagligt fokus	Risiko-analyse i samfunds-kontekst	Politisk og juridisk styring	Metodisk og etisk efterretnings ledelse	Efterretnings-analyse	Governance af cyber- og informations-sikkerhed	Fremtids-analyse	Tværfag-lighed og fleksible valgfag
Professionel master							
Master i Intelligence og Cyber Studier (SDU, FAK)	X	X	X	X	X	X	X
Master of Cyber Security (DTU)	(X) IT-fokuseret				X	(X) IT-fokuseret	
Master i it, softwarekonstruktion med specialisering i it-sikkerhed (AU, SDU, AAU)					X		(X) IT-fokuseret
Fuldtidsstudier							
Kandidat i Seucurity and Risk Management (KU)	X		(X) Intelligence som enkelt valgfag	(X) Intelligence som enkelt valgfag			X
Professionsbachelor som Katastrofe- og risikomanager (KP)	(X) intet fokus på cyber eller efterretning	(X) intet fokus på cyber eller efter-retning				(X) intet fokus på cyber eller efter-retning	
Diplomuddannelse							
IT-diplomuddannelsen med Cyber defence-kursusforløb (DTU)		(X) IT-foku-seret			(X) IT-fokuseret		(X) IT-fokuseret
Diplom i it-sikkerhed (EA, KEA)					(X) IT-fokuseret		(X) IT-fokuseret
Opkvalificering							
Junior Cyberanalytiker hos Cyberakademiet (12 uger med løn hos CfCS)	?	?	X	X	?	?	

* Tabellen benytter Master i Intelligence og Cyber Studier (MICS) som referencepunkt og afsøger derigennem tilnærmende uddannelsers indhold. Hvor fagindholdet overlapper på et overordnet plan, benyttes et X og den grønne farve, mens et (X) og en gulfarvet celle med en kort forklaring angiver et noget mindre overlap. Hvide felter betyder minimalt eller intet overlap. Uddannelserne er grupperet efter niveau, hvilket også skal tages med i overvejelserne, da en gul celle under professionel master og eksempelvis diplomuddannelse ikke nødvendigvis er umiddelbart sammenlignelige.

** Den sammenlignende analyse er baseret på en gennemgang af uddannelsernes egne præsentationer på nettet.

3.1. Et unikt samarbejde mellem SDU og FAK

Ovenstående tabel viser, at MICS med sin særlige fagkombination bringer en unik uddannelse på markedet, der ikke direkte bliver matchet af andre sammenlignelige udbud. MICS åbner dermed for en ny type kvalificering og potentielt nye stillingskategorier uden at forringe andre uddannelsers vilkår. MICS imødekommer et anerkendt behov på markedet, der hidtil ikke er opdyrket og udbudt i en dansk kontekst og afspejler et bredspektret kompetencebehov, som beslægtede uddannelser ikke i samme grad adresserer. Det særlige samarbejde mellem SDU og FAK udfylder derfor et tomrum, som andre uddannelser tilnærmer sig fra anderledes specialiserede og særligt tekniske vinkler – eller uddannelser, der hidtil har henvendt sig direkte til Forsvarets ansatte gennem enkeltstående kurser eller til klassiske fuldtidsstuderende.

3.2. Berøringsflader til andre uddannelser

Da der ikke findes nogen direkte beslægtede eller konkurrerende uddannelser til MICS i Danmark på hverken det professionelle master-niveau eller som fuldtidsstudieudbud, orienterer den ovenstående sammenligning sig i stedet til beslægtede uddannelser ved at selektere på overlap med dele af MICS' faglige fokus. Der findes tre store berøringsflader til tilnærmende uddannelser, der i forskellig grad udgøres af henholdsvis:

1. efterretningsanalyse og -ledelse
2. governance/styring af de to domæner - cyber- og informationssikkerhed
3. risikoanalyse- og strategisk planlægning og management

Graden af overlap med MICS er hovedsageligt betinget af uddannelsernes teknik- og efterretningssigte samt deres uddannelsesspecialisering.

- **Tekniske cybersikkerhedskompetencer**: Der findes et konsolideret marked for master-uddannelser fokuseret på de tekniske og projektledelsesmæssige aspekter af IT- og cybersikkerhed, hvor IT-systemarkitektur, IT-sikkerhedspolitikker og programudvikling af høj teknisk karakter udbydes. Danmarks Tekniske Universitet udbyder eksempelvis den engelsksprogede to-årige *Master of Cyber Security*, der henvender sig til IT-professionelle og har et konkret teknisk fokus på IT-systemers sikkerhed. Et lignende fokus kan findes på den to-årige Master i IT, der udbydes i samarbejde mellem Aarhus Universitet, Syddansk Universitet og Aalborg Universitet, hvor kursisterne kan vælge fagpakken "*softwarekonstruktion med specialisering i it-sikkerhed*." Uddannelsesoversigtens sammenligning tydeliggør, hvordan især det efterretningsmæssige aspekt er fraværende i disse to master-uddannelser.

- **Efterretningskompetencer:** Den mere praksisnære efterretningstilgang har næsten udelukkende været udbudt i Forsvarets regi, som eksempelvis *Myndighedsfælles Efterretningsanalytikerkursus 2020* (7,5 ECTS) og *Master i Militære Studier* med modulet *Værnsfælles Videregående Efterretningsuddannelse (VF-E)*, der tillader maksimalt 20% civile studerende blandt max-optaget på 30 i alt. Derudover udbyder Forsvarets Efterretningstjeneste et teknisk orienteret 12 ugers lønnet kursus som junior cyberanalytiker til mulig videre ansættelse i Cybersituationscenteret under FE. Der er således både begrænset udbud og adgang til efterretningsorienteret uddannelse og ingen af disse muligheder eksisterer på professionel master-niveau.

- **Uddannelsesspecialisering:** De eksisterende master-uddannelser i cybersikkerhed dækker ikke det efterretningsmæssige sigte for MICS, mens de eksisterende efterretningsuddannelser

ikke dækker det brede akademiske sigte for MICS. Københavns Universitet udbyder en engelsksproget kandidatuddannelse på 120 ECTS i *Security and Risk Management*, der har visse overlap med MICS ved at opbygge risikoanalytiske evner og udbyde faget *Intelligence* (7,5 ECTS). Denne uddannelse er dog et fuldtidsstudie og ikke en master og indeholder ikke det praktiske og anvendelige element, der kendetegner MICS.

- **Enkeltkurser:** Den kvalitative behovsanalyse har udover at pege på nogle af de ovenstående uddannelser også afdækket, at man blandt aftagerne benytter kortere kurser, der kompetencemæssigt har visse overlap med MICS. Det drejer sig f.eks. om NATOs *Cooperative Cyber Defence Centre of Excellence* i Estland, der udbyder kurser af få dages varighed til et begrænset antal personer fra medlemsstater. I forlængelse af efterretningssporet er eksempelvis Politiets Efterretningstjenestes fire-timers lange *Projekt Insider* kursus blevet nævnt. Udpegningen af disse enkeltstående kurser understreger på samme tid behovet for kursernes faglige indhold, men også den manglende uddannelsesmæssige ramme om dette indhold. En ramme, som MICS leverer og placerer i et højt kvalificeret forskningsmiljø.

4. Baggrund for behovsanalysen

Behovsafdækningen har fundet sted gennem to spor, der består af henholdsvis spor 1: det forsvars- og politimæssige myndighedsspor, med Forsvarets Efterretningstjeneste; Politiets Efterretningstjeneste og Forsvaret som aftagere og respondenter og spor 2: det offentlig-private sikkerhedsspor, med relevante virksomheder og civile styrelser og organisationer som aftagere og respondenter. De to spor inkorporerer den udprægede grad af myndigheders samarbejde med, samt udlicitering til, private IT- og cybersikkerhedsaktører.[3] Behovsafdækningen for spor 1 er foretaget gennem analyser udført af Forsvarsakademiet i samarbejde med efterretningstjenesterne og efterfølgende behovstilkendegivelser fra ledelsesniveau. Behovsafdækningen for spor 2 er udført af SDU via kvalitative interviews og en spørgeskemaundersøgelse. Udviklingen af uddannelsen har prioriteret at MICS fastholder sin oprindelse i behov fra aftagerne i spor 1 og balancerer med relevans og appel til aftagere i spor 2. Behovsanalysens to spor er udtryk for et ønske om både at sikre vidensdeling og kompetenceombygning bredt i samfundet samt langsigtet rentabilitet for MICS ved at optage studerende fra forskellige sektorer.

4.1. Et højnet trusselsniveau driver et øget behov for MICS-kompetencer

Det er vigtigt at undersøge både de generelle samfundsmæssige og rammegivende tendenser, der driver efterspørgslen på MICS, og de helt konkrete behov hos aftagerne. Derfor præsenteres først et helikopterperspektiv og dernæst går analysen i dybden med behovsanalyserne fra spor 1 og 2.

[3] MICS kvalificerer studerende til at forstå og facilitere sikkerhedsbevidst offentlig-privat samarbejde om udvikling og drift af IT-projekter ved at sikre inddragelse af brede trusselsbilleder. Offentlig-privat samarbejde i det digitale domæne har et stort sikkerhedsfokuseret styringsbehov, da disse er præget af særlige problemstillinger ift. ansvarsfordelingen mellem det politiske og administrative niveau og forholdet til private aktørers rolle i og forpligtelser for national sikkerhed. Se fx Madeline Carr (2016) "Public–private partnerships in national cyber-security strategies", *International Affairs*: https://www.chathamhouse.org/sites/default/files/publications/ia/INTA92_1_03_Carr.pdf , Digitaliseringsstyrelsen (2016): *Kodeks for det gode kunde-leverandørsamarbejde*: https://digst.dk/media/12625/kodeks-for-godt-kundeleverandrsamarbejde-i-staten.pdf og *National strategi for cyber- og informationssikkerheds* initiativ 2.4 "Erhvervspartnerskab for øget it-sikkerhed i dansk erhvervsliv" som eksempelvis udmøntet gennem Erhvervsministeriets indsatser https://em.dk/nyhedsarkiv/2018/maj/regeringen-styrker-indsatsen-for-at-oege-it-sikkerhed-i-smaa-og-mellemstore-virksomheder/

Det seneste forsvarsforlig 2018-2023 har afsat 1,5 mia. kroner til Danmarks digitale sikkerhed[4], der blandt andet udmøntes gennem 25 initiativer i "*National Strategi for Cyber- og Informationssikkerhed 2018-2021*".[5] Forsvarsforliget reflekterer et akut og stigende behov for kombinationen af cybersikkerheds- og efterretningskompetencer i en bred vifte af danske private og offentlige sektorer. Et højnet trusselsniveau udgøres af både statslige og ikke-statslige aktører, der vedvarende og tilpasningsdygtigt udfordrer cybersikkerheden og den bredere modstandsdygtighed/resilience hos alle samfundsmæssige aktører. De potentielle samfundsmæssige sårbarheder stiger i takt med at stater øger og udnytter digitaliseringens fordele. I Danmark har Center for Cybersikkerhed (CfCS) under Forsvarets Efterretningstjeneste vurderet at "*Cybertruslen er en alvorlig trussel mod Danmark. Cyberangreb har især økonomiske og politiske konsekvenser.*"[6]

Den nationale strategi for cyber- og informationssikkerhed identificerer en række sektorer (energi-, transport-, tele-, finans-, sundheds-, og søfartssektoren), der anses for at være særligt kritiske og som så hurtigt som muligt vil skulle oparbejde styrkede cybersikkerheds-kompetencer. Disse har hver især udviklet sektorstrategier med konkrete krav om standardisering, styring og overvågning. Strategierne stiller blandt andet større krav til sektorens egen kortlægning af sårbarheder og kritisk infrastruktur, sektorberedskab og vidensdeling.[7] De kritiske sektorer indgår i samspil med en lang række aktører i komplekse værdi- og forsyningskæder, der stiller fortsat større krav til efterretnings- og cyberanalytiske kapaciteter. CfCS peger eksempelvis specifikt på cybertruslen mod IT-serviceudbydere og deres kunder, HR-afdelinger og angreb via LinkedIn samt danskflagede skibes operationelle systemer.[8] Behovet for MICS-kompetencer drives således frem af en kombination af internationale og nationale politiske svar på cybertrusler, der spænder fra NATO[9] over EU[10] til skiftende danske regeringer samt et lokalt forretningsdrevet momentum der spænder fra kommune til internationale

[4] Ritzau (2018): "Regeringen vil bruge 1,5 milliarder på cyberforsvar", *Berlingske.dk* https://www.berlingske.dk/politik/regeringen-vil-bruge-15-milliarder-paa-cyberforsvar

[5] MICS-uddannelsen flugter tæt med National strategi for cyber- og informationssikkerheds tre pejlemærker ved at udbyde brede faglige kompetencesæt til brug for både kritiske sektorspecifikke stillinger og overordnet sikkerhedsledelse, der fanges under 1. Tryg hverdag, 2. Bedre kompetencer og 3. Fælles indsats. Uddybende detaljeret kan findes på https://digst.dk/strategier/cyber-og-informationssikkerhed/

[6] Center for Cybersikkerhed (2020): *Trusselsvurdering 2020: Cybertruslen mod Danmark*, s. 3. Trusselsvurderingen understreger at *"Truslen fra cyberkriminalitet er MEGET HØJ. Truslen er rettet mod alle*" samt "*Truslen fra cyberspionage er MEGET HØJ. Truslen er især rettet mod myndigheder, som arbejder med udenrigs- og sikkerhedspolitik, samt virksomheder, der besidder en viden, som andre stater har interesse i.*" https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/-cybertruslen-mod-danmark-2020-.pdf

[7] Se fx Finanssektorens delstrategi: Finanstilsynet (2019): *Strategi for den finansielle sektors cyber- og informationssikkerhed 2019 – 2021*, s. 3 https://em.dk/media/12278/delstrategi-for-finanssektorens-cyber-og-informationssikkerhed_.pdf

[8] Center for Cybersikkerhed (2020): *Trusselsvurdering: Cybertruslen mod it-serviceudbydere* https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cfcs-trusselsvurdering-cybertruslen-mod-it-serviceudbydere.pdf; *Trusselsvurdering: HR-afdelinger rammes også af målrettede cyberangreb* https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cfcs-trusselsvurdering-cybertruslen-mod-hr-afdelinger.pdf; *Trusselsvurdering: Cybertruslen mod skibes operationelle systemer* https://cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/cybertruslen-mod-skibes-operationelle-systemer.pdf

[9] NATO erklærede i 2016 cyberspace for et selvstændigt militært domæne på lige fod med luft, land og vand og stiller derfor øgede krav til medlemsstaternes kapabiliteter. En væsentlig del af det danske svar på denne efterspørgsel er opbygningen af en operationel offensiv cyberkapacitet, der stilles til rådighed for NATO og samtidigt potentielt øger risikoen for angreb mod Danmark. Se fx Mikkel Storm Jensen (2020): "Småstater og cybervåben – nye muligheder og nye begrænsninger", *Økonomi og politik* nr. 3, 2020 https://www.djoef-forlag.dk/openaccess/oep/files/2020/3_2020/3_2020_4.pdf

[10] EU's direktiv om sikkerhed for net- og informationssystemer (NIS-direktivet) stiller øgede sikkerhedskrav til " *navnlig forsyningsvirksomheder, offentlige myndigheder m.fl. i sundhedssektoren og andre operatører af væsentlige tjenester*", hvilket blandet andet indebærer udarbejdelser af risikovurderinger og -styring. Se fx Mads Nygaard Madsen, Charlotte Kunckel og Maria Pilh Arendsdorf Bengtsen (2018): "Implementering af NIS-direktivet: nye krav til sikkerheden i net- og informationssystemer", *Ret & indsigt*, nr. 4, 2018 https://www.horten.dk/viden/artikler-2018/implementering-af-nis-direktivet

virksomheder og kritiske serviceudbydere om modstandsdygtighed/resilience og evne til at holde forretningen kørende (*business continuity)*. Evnen til analytisk at forudse, undgå eller i videst muligt omfang minimere cybertrusler og deres effekter er derfor en voksende konkurrenceparameter for både politiske og private aktører, der ønsker at skabe tryghed og stabilitet for henholdsvis borgere og kunder.

Institutionelle svar på det højnede trusselsniveau indebærer kommende lovgivning om investeringsscreening af de kritiske sektorers infrastruktur. Det stiller nye krav til detaljeret efterforskning af ejerskabsforhold, værdi- og forsyningskæder samt leverandørstyring i relationen til udenlandske aktører.[11] Derudover vil regeringen etablere en ny national efterforskningsenhed i politiet, der samler otte nuværende enheder – herunder Nationalt Cyber Crime Center (NC3) og Landsdækkende Center for It-relateret økonomisk Kriminalitet (LCIK). Den nye 800-mand store enhed skal styrke kompleks efterforskning og anvendelse af nye teknologier.[12] Disse udviklingstendenser peger på et behov for tættere koordination mellem efterretningstjenesterne og resten af samfundet. MICS vil bidrage til denne koordination gennem vidensdeling, kompetenceopbygning og ny forskning indenfor intelligence og cyber områderne.[13] Målet er sikring af gensidig faglig kompatibilitet hos både leverandør og aftager af efterretninger samt på netværksdannelse under uddannelsen.

MICS er relevant for en bred gruppe af aftagere, der arbejder med cyber- og informationssikkerhed, men grundet uddannelsens oprindelse som et svar på forsvars- og politimyndigheders behov, giver det mening af skelne mellem disse og andre samfundsaktører.

4.2. Efterspørgsel fra myndighedsområder i vækst

Aftagerne hos forsvars- og politimyndighederne gennemgås i det følgende. Efterretningstjenesterne arbejder hovedsageligt under klassificerede forhold og der kan kun i begrænset omfang og ved hjælp af få offentlige kilder redegøres for udviklingstendenser af interesse for MICS. Det står dog klart at Forsvarets Efterretningstjeneste over de seneste fem år har oplevet en betydelig ressourcemæssig tilgang i form af stigende bevillinger. På finansloven fra 2015 lød tjenestens bevilling på 675 mio. kr., mens den i 2019 var vokset til i alt 972 mio. kr. Det seneste forsvarsforlig sikrede yderligere tilgang af midler, så FE's årlige bevilling ved udgangen af forligsperioden i 2023 forventes at være på cirka 1,1 mia. kr. De tildelte forsvarsforligsmidler stiger fra 34 mio. kr. i 2018 til 230 mio. i 2023 og "*vil primært skulle styrke FE's evne til at imødegå cybertrusler, men der er også afsat midler til at imødegå påvirkningsoperationer mod Danmark fra fremmede stater og til at sikre FE's fortsatte teknologiske udvikling*."[14] FE oplyser af sikkerhedsmæssige årsager ikke antallet af medarbejdere, men der sker en

[11] Camilla C. Collet, Anne-Kathrine Holstein (2019): *Screening af udenlandske investeringer – nye regler på vej*, Gorrissen Federspiel https://gorrissenfederspiel.com/viden/nyheder/screening-af-udenlandske-investeringer-nye-regler-paa-vej ; Kromann Reumert (2020): *Forslag til gennem-gribende ny investerings-screenings-lov sendt i høring* https://www.kromannreumert.com/Nyheder/2020/12/Forslag-til-gennemgribende-ny-investeringsscreeningslov-sendt-i-hoering

[12] Regeringen (2020): Trygheden først – Et politi der er dér, hvor danskerne har brug for det. Regeringens oplæg til aftale om politiets og anklagemyndighedens økonomi 2021-2024, s. 17-18 https://www.regeringen.dk/media/9876/fleraarsaftale-udspil-endelig.pdf; Søren Domino, Jens Beck Nielsen (2020): *Nick Hækkerup vil skabe et dansk kraftcenter for efterforskning: »Jeg drømmer om, at vi kan finde en forkortelse, der passer med F.B.I.«*, Berlingske 21. august https://www.berlingske.dk/politik/nick-haekkerup-vil-skabe-et-dansk-kraftcenter-for-efterforskning-jeg ; Regeringen (2020): *Aftale om politiets og anklagemyndighedens økonomi 2021-2023*, s. 14 https://www.justitsministeriet.dk/wp-content/uploads/2020/12/Aftale-om-politiets-og-anklagemyndighedens-oekonomi-2021-2023-1.pdf

[13] Begge forskningsinstitutioner er i proces med at ansætte forskere som led i at styrke et aktivt forskningsmiljø og forskningsbaseret undervisning indenfor rammerne af MICS-uddannelsen.

[14] Forsvarets Efterretningstjeneste (2019): *Indblik: Vores viden og indsats — Danmarks sikkerhed. Forsvarets Efterretningstjenestes beretning 2017-2018*, s. 37 https://fe-ddis.dk/globalassets/fe/dokumenter/2019/-fe-beretning-2017-18-2019.pdf

tilgang. Samtidigt stiger andelen af medarbejdere i FE, der har cyber som overordnet fokusområde, så status ved udgangen af 2018 var, at 30% arbejder med cybersikkerhed og 14% med CNO (populært kaldet hackeraktiviteter).[15] Vendes blikket mod Politiets Efterretningstjeneste observeres en lignende tendens, hvor bevillingens størrelse er vokset fra 580 mio. kr. i 2015 til 890 mio. kr. i 2020.[16] Sammenlagt lægger analysen disse offentligt tilgængelige oplysninger til grund for at konkludere, at efterspørgslen fra disse myndighedsområder for en uddannelse som MICS, vil være i vækst.

4.3. Civile samfundsaktørers behov for stærkere cyberkompetencer

MICS er som en samfundsvidenskabelig og ikke-teknisk specialiseret uddannelse relevant for en bred gruppe af professionelle lige fra analytikeren til lederen. Relevansen gælder eksempelvis også personer i stillinger, hvor emner som cyber- og informationssikkerhed hidtil har været underprioriterede. Derfor flugter det med motivationen for MICS, at denne udfordring er en topprioritet for næste version af *National strategi for cyber- og informationssikkerhed,* da kommissoriet vægter ledelsesforankring og kompetenceopbygning som tema nummer ét. Herunder understreges også en styrket indsats på uddannelsesområdet. Strategien kommer til at indeholde initiativer, der skal "*sikre en vedvarende topledelsesmæssig, forståelse, forankring og prioritering af cyber- og informationssikkerhed, samt en større videns- og awarenessindsats rettet mod ledere og medarbejdere i statslige myndigheder og virksomheder, også ift. de tekniske tiltag*".[17]

Konkret er der et akut behov for, at ledere får opbygget kompetencen til at forstå sammenhængen mellem de mere tekniske aspekter og det bredere trusselsbillede for dermed at kunne sikre solidt funderede beslutningssituationer. Udfordringen understreges af Deloittes *Cyber Risk Landscape Report 2019*, der finder at 26% af de undersøgte ledere aldrig eller kun sjældent bliver underrettet om status på cybersikkerhed.[18] Den manglende topledelsesforankring har givet anledning til, at f.eks. Bestyrelsesforeningen i samarbejde med en række cybersikkerhedsaktører og støttet af Industriens Fond, udbyder korte kurser og andre uddannelsesaktiviteter for bestyrelsesmedlemmer.[19] Samfundsvidenskabelige MICS-kompetencer i rummet mellem teknik, analyse og strategi finder ifølge interesseorganisationen for danske IT-professionelle, Dansk IT, også stor anvendelse under ledelsesniveauet i takt med at organisationer bliver mere datadrevne.[20] Sammenlagt lægger analysen disse overordnede perspektiver til grund for at konkludere, at der sker en stigning i behovet for at kvalificere de analytiske cybersikkerhedskompetencer fra topledelse til medarbejderniveau.

5. Baggrunden for to separate behovsanalyser

Behovsanalysen bevæger sig nu væk fra de overordnede behovsdrivende udviklinger over til de konkrete undersøgelser af henholdsvis spor 1, forsvars- og politimyndigheder, og spor 2, offentlig-privat sikkerhedsspor. Klassificering af oplysninger sætter rammerne for detaljeringsgraden af

[15] Ibid., s. 27

[16] Finansministeriet (2020): *Forslag til finanslov for finansåret 2021*, 11.23.16. Politiets Efterretningstjeneste, s. 56 https://fm.dk/media/18181/ffl21a.pdf

[17] Forsvarsministeriet (2020): *Kommissorium for udarbejdelse af en ny national strategi for cyber- og informationssikkerhe*d, s. 4-5 https://fmn.dk/globalassets/fmn/dokumenter/nyheder/-kommissorium-cyberstrategi-fra-2021-.pdf

[18] Deloitte (2019): *Hacks me, hacks me not… Cybersecurity is the Achilles heel of Danish businesses - Cyber Risk Landscape Report 2019* https://www2.deloitte.com/dk/da/pages/about-deloitte/pressemeddelelser/topledere-mangler-fokus-paa-cyber-sikkerhed.html

[19] Bestyrelsesforeningen (2019): *Styrkelse af Strategiske Cyberkompetencer* https://bestyrelsesforeningen.dk/styrkelse-af-strategiske-cyberkompetencer/

[20] Kim Stensdal (2020): *Data kan styrke danske virksomheder – men formlen på succes handler ikke om teknologi*, BusinessInsights https://www.businessinsights.dk/digitalisering/data-kan-styrke-danske-virksomheder-men-formlen-paa-succes-handler-ikke-om-teknologi/

behovsanalysen i spor 1 og derfor gengives i det følgende alene den overordnede interne afklaringsproces. Spor 2 har haft mulighed for at tilgå behovsafklaringen gennem en mere åben tilgang og afrapporteres mere detaljeret. Begge analyser har informeret og formet tilrettelæggelsen af MICS i forhold til de faglige og praktiske kompetencebehov, der efterspørges.

Det er en prioritet at kalibrere uddannelsens relevans i forhold til både aktuel og fremtidig efterspørgsel hos flere slags aftagere (deraf de to spor), for at øge rentabilitet og yde et bredt samfundsmæssigt bidrag.

6. Behovsanalyse spor 1: Behov for MICS-uddannelsen inden for forsvars- og politiområdet

Det operative behov for efterretnings- og cyberuddannelser inden for politi- og forsvarsområdet er blevet afdækket af Forsvarsakademiet, både generelt og konkret i 2020.

Helt overordnet set vil uddannelsessamarbejdet støtte et af Forsvarsministerens prioritetsområder og have en positiv, afledt effekt på en række initiativer, der forventes igangsat inden for cyber-området. Derudover vil det støtte en tværministeriel tankegang inden for et nyt og efterspurgt vidensområde i hastig udvikling.

Inden for Forsvaret henvender uddannelsen sig til især yngre officerer og andre, der gennem deres virke og funktion har behov for uddannelse på de to områder. Herved får Forsvaret den størst mulige nytte af de tildelte kompetencer og den enkelte soldat har mulighed for at gennemføre et karriereforløb på områder, hvor Forsvaret vil få større og større behov for viden og kompetencer.

6.1. Generelt behov for cyberuddannelser

Hvad angår det generelle behov for cyberuddannelser inden for Forsvaret, har Forsvarsministeriet udpeget cyberdomænet som et indsatsområde, der vil vokse i både ministeriet, Forsvaret, Forsvarets Efterretningstjeneste og ved Politiets Efterretningstjeneste. Danmark har derfor opbygget cyberkapaciteter som en del af det samlede forsvar, og i 2020 færdiggjorde det første hold af cyberværnepligtige deres uddannelse.[21]

Imidlertid eksisterer der ikke en uddannelse på cyberdomænet, der har øje for den sikkerhedspolitiske kontekst samt har både et globalt og et skandinavisk perspektiv. Derfor er der et behov for specialiseret uddannelse på området, der dækker forståelsen for domænets muligheder og begrænsninger.

6.2. Generelt behov for efterretningsuddannelser

Hvad angår det generelle behov for efterretningsuddannelser inden for Forsvaret, har Forsvarsakademiet i 2020 gennemført en analyse af sammenhængen mellem operative opgaver og uddannelsesbehov indenfor efterretningsområdet med henblik på at identificere mulige optimeringer og anbefalinger til efterretningsuddannelse indenfor Forsvarskommandoens myndighedsområde.

Analysen tager afsæt i en kortlægning af eksisterende efterretningsuddannelser, sammenhæng imellem disse, samt vurdering af hvorvidt eksisterende uddannelser understøtter aktuelle og fremtidige operative opgaver.

[21] Cyberværnepligten leverer færdiguddannede til videre karriere og uddannelse i både den civile og militære sektor og Forsvaret tilknytter selv en del af disse, for hvem MICS fremadrettet vil være kvalificerende. Ritzau (2020): *Første hold cyberværnepligtige bliver attraktive for erhvervslivet*: https://sn.dk/Danmark/Foerste-hold-cybervaernepligtige-bliver-attraktive-for-erhvervslivet/artikel/1387676

Én af analysens anbefalinger er, at FAK udbyder værnsfælles og myndighedsfælles videreuddannelse på masterniveau. Dette blandt andet med henblik på at styrke uddannelse i principperne bag og effekten af efterretningsdrevne militære operationer og tilsikre interoperabilitet på tværs af værnene i Forsvaret og andre myndigheder.

6.3. Konkret behov for Master i Intelligence og Cyber Studier

Hvad angår det konkrete behov for Master i Intelligence og Cyber Studier, har Forsvarsakademiet i den afklarende fase været i kontakt med en række aftagende myndigheder inden for politi- og forsvarsområdet:

- Politiets Efterretningstjeneste
- Forsvarets Efterretningstjeneste
- Forsvarskommandoen
- Forsvarsministeriets Materiel- og Indkøbsstyrelse

Alle aftagere har modtaget uddannelsesbeskrivelsen (den samlede uddannelses formål og indhold samt modulernes beskrivelser), og der er også afholdt et uddybende møde med de centrale aftagere. Samlet set er der fra de nævnte myndigheder tilkendegivet et årligt, konkret behov for op til 13-15 studerende på hele uddannelsen og mindst 6-7 studerende på enkeltmoduler. Alle aftagerne har vurderet et generelt behov for uddannelsen. Dette gælder også de aftagere, der ikke har kunnet sætte konkrete tal på deres eget behov. Nedenfor ses oversigt over de myndigheder inden for politi og forsvar, FAK har været i dialog med, hvilken dokumentation de har modtaget, samt hvilke tilkendegivelser af behov for uddannelsen, de har angivet.

Myndighed/aftager	Dokumentation modtaget	Tilkendegivelse af behov
Politiets Efterretningstjeneste	Uddannelsesbeskrivelse (formål og indhold samt modulbeskrivelser) Møde med dekanerne for SDU-SAMF og FAK.	Tilkendegivelse af et årligt behov for 2-3 studerende på hele uddannelsen og ca. 5 studerende på enkeltmoduler.
Forsvarets Efterretningstjeneste	Uddannelsesbeskrivelse (formål og indhold samt modulbeskrivelser) Møde med dekanen for FAK.	Tilkendegivelse af et årligt behov for 1-2 studerende på hele uddannelsen og 1-2 studerende på enkeltmoduler årligt
Forsvarskommandoen	Uddannelsesbeskrivelse (formål og indhold samt modulbeskrivelser) Uddybende notat og møde med FAK.	Godkendelse af, at FAK kan indgå i samarbejdet, og at der er behov for uddannelsen i myndighederne under Forsvarskommandoen. Tilkendegivelse af et årligt behov for op til 10 studerende på hele uddannelsen eller på enkeltmoduler.
Forsvarsministeriets Materiel- og Indkøbsstyrelse	Uddannelsesbeskrivelse (formål og indhold samt modulbeskrivelser)	Tilkendegivelse af generel interesse og behov for uddannelsen. Ingen tilkendegivelse af et konkret, årligt behov for et antal studerende.

7. Behovsanalyse spor 2: Behov for MICS-uddannelsen i det offentlig-private sikkerhedsspor

Kortlægningen af behovet for MICS-kompetencer i det offentlig-private sikkerhedsspor har givet værdifuldt input til justeringer af fokus, fagligt indhold og i særlig grad uddannelsens sproglige udbud til også at omfatte en engelsk version. Behovsanalysens formål har været at afdække aftagernes praktiske ønsker til kompetencer og derpå matche disse med en høj akademisk standard.

7.1. Behovsanalysens metode og respondenter: Kvalitative interviews

Dataindsamlingen er foregået i to etaper, der bestod af henholdsvis 1) semistrukturerede kvalitative interviews med en række vægtige sektor- og brancherepræsentanter og 2) en større kvantitativ surveyundersøgelse. Udvælgelsen af respondenter har fundet inspiration i National strategi for cyber- og informationssikkerheds udpegning af seks kritiske sektorer: sundhed, finans, tele, søfart, transport og energi. Disse er brugt til at fokusere samt sikre bredde i respondentrepræsentationen.

Respondenterne er alle centralt placerede personer, der beskæftiger sig med cyber- og/eller informationssikkerhed samt risikostyring og som har professionel erfaring fra en række stillinger fordelt mellem både den offentlige og private sektor. En del af de interviewede har skiftet job fra Forsvarets Efterretningstjeneste og Center for Cybersikkerhed til deres nuværende stillinger. Dermed besidder respondenterne de nødvendige kompetencer til at kunne bedømme MICS' potentiale og faglige indhold. En omfattende afsøgning, inden udvælgelse af respondenterne, er foretaget ved at gennemse mediedækning af cyber- og informationssikkerhed, konsultere brancheorganisationer, store virksomheder og centrale myndigheder. LinkedIn er brugt til at gennemgå respondenternes baggrund.

Analysen har især draget fordel af at få svar fra de forskellige sektorer. Eksempelvis har tre ud af seks DCIS-sektoransvarlige (den Decentrale enhed for Cyber- og Informationssikkerhed for hver af de kritiske sektorer fungerer som forbindelsesled til Center for Cybersikkerhed) medvirket sammen med brancherepræsentanter og store virksomheder såvel som myndigheder hjemhørende i de kritiske sektorer. Der kan således argumenteres for, at respondentlisten dækker og repræsenterer en meget stor del af de personalegrupper, der i Danmark er beskæftiget indenfor cyber- og informationssikkerhed.

De 12 kvalitative interviews med i alt 14 respondenter er gennemført via videomøder med en varighed på mellem 30 minutter og en time. Respondenterne er blevet præsenteret for uddannelsens overordnede udformning og faglige indhold og bedt om på denne baggrund at behovsvurdere efterspørgsel samt give konstruktiv kritik og forslag til ændringer. Processen har været særdeles informativ i forhold til MICS og har samtidigt informeret den efterfølgende elektroniske survey.

Respondentliste fra kvalitative interviews

Navn	Titel	Organisation
Malene Hein Nybroe	Enhedschef, Center for undergrund og beredskab	Energistyrelsen
Søren Bank-Greenfield	Head of Sund-DCIS, Afdelingschef	Sundhedsdatastyrelsen
Sine Tarby Christensen	Senior Corporate Incident & Crisis Manager	A.P. Møller - Mærsk
Tim Sloth Jørgensen	Tidligere forsvarschef, programchef, Industriens Fonds Cyberindsats	Industriens Fond
Malene Stidsen	Projektleder, Industriens Fonds Cyberindsats	Industriens Fond
Anders Balling	Head of Finans-DCIS, underdirektør Finanstilsynet	Finanstilsynet
Niklas Høegh-Guldberg	Senior Director, Solutions, Architects & Design	TDC Group Security
Astrid Gufler	Politisk chefrådgiver, Djøfs TechDK Kommission	DJØF
Morten Rosted Vang	Fagleder, Digital ansvarlighed og cybersikkerhed	Dansk Industri
Dennis Larting	Head of Tele-DCIS	DKCERT/DTU
Lotte Hviid Melsen	Teamleder, Digital Sikkerhed i kontor Digital vækst	Erhvervsstyrelsen
Martha Sophie Halkjær Ingvorsen	Fuldmægtig, Digital Sikkerhed i kontor Digital vækst	Erhvervsstyrelsen
Thomas Flarup	Executive Vice President, Technology & Security Services	KMD
Mads Halkjær Ingvorsen	Senior Manager, Cyber Intelligence Centre	Deloitte

* DCIS er den Decentrale enhed for Cyber- og Informationssikkerhed, der er oprettet for hver af de seks samfundskritiske sektorer identificeret i regeringens *National Strategi for Cyber- og Informationssikkerhed 2018-2021*. DCIS er et samlingspunkt for sektorens trusselsvurderinger, overvågning og kontakt til Center for Cybersikkerhed.

8. Behovsanalysens metode og respondenter: Elektronisk survey

Besvarelserne fra de kvalitative interviews har fungeret som udgangspunkt for spørgsmål i den elektroniske survey og respondenterne er udvalgt efter samme fremgangsmåde. Surveyen er distribueret via henholdsvis mail og LinkedIn til i alt 135 personer inklusive respondenterne fra de kvalitative interviews. Responsraten er med 54 gennemførte svar på 40%, hvilket er meget tilfredsstillende.[22] Surveyen blev ledsaget af en én-sides flyer med overordnede informationer om MICS og med opfølgende oplysninger i selve spørgeskemaet. Formålet var dels at få mere bredde i

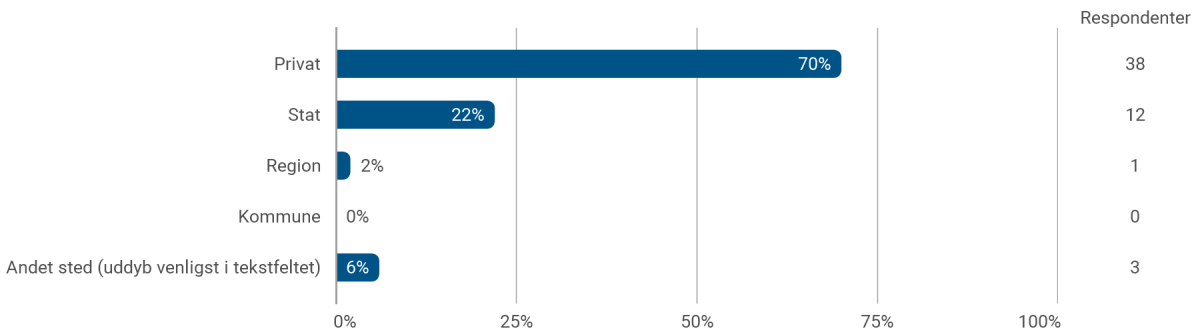
[22] Responsraten er sandsynligvis lidt lavere, da nogle respondenter per instruktion har videresendt til personer i lignende stillinger som deres egen, men ikke har informeret om hvem og hvor mange, de har kontaktet. Antallet vurderes dog at være begrænset.

respondenters besvarelser end det er muligt med kvalitative interviews og at spørge mere direkte ind til konkrete præferencer. Nedenstående oversigt angiver respondenternes karakteristika.

Respondentliste fra elektronisk survey: Stillingsbetegnelser

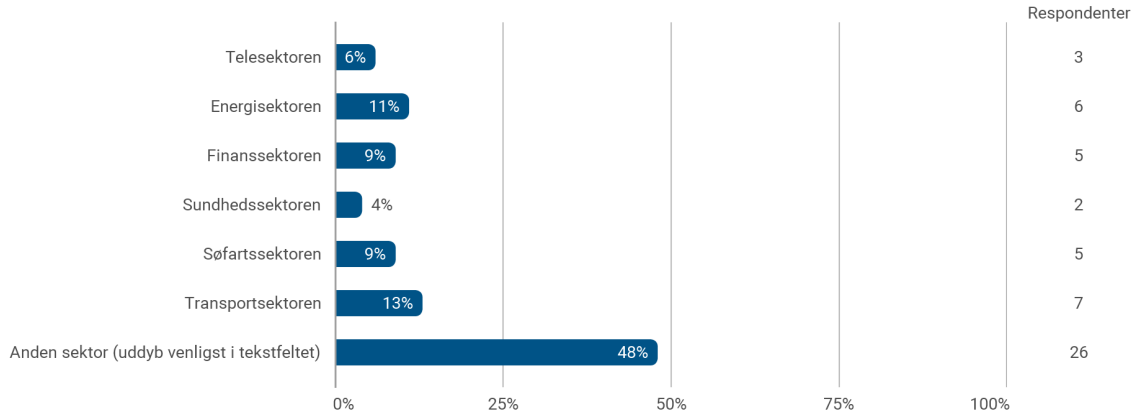
54 gennemførte besvarelser		
Politisk konsulent	IT-Chef	Direktør
Uddannelseschef	Chef for IT-afdelingen	Head of Security
CDO	Risk Manager	Ciso
Direktør	CIO/IT Direktør	EVP, Driftsdirektør
programchef	Fuldmægtig	Projektdirektør
Politisk chefrådgiver	CISO	CRO
Uddannelses og forskningspolitisk chef	Programleder	Leder af [fjernet for at sikre anonymitet]-sikkerhedsenhed
Head of branding og marketing	Dansk informationssikkerhedschef	CISO
Director, Group Security	CTO	kontorchef
Key Account Manager	Afdelingschef	Senior Management
Forsknings og teknologidirektør	CISO	IT Chef
Områdechef	fuldmægtig	Assoc. Director Information Security
Konsulentansvarlig	Direktør	Chef for sikkerheds- og identitetstjenester
Group Security Manager	kontorchef	CISO
Projektleder	DPO	Managing Partner
Crisis Manager	CISO	CISO
CEO	kontorchef	Leder i en strategisk cyber funktion
Adm. direktør	[fjernet for at sikre anonymitet] IT Manager	CISO

Hvor er du ansat?[23]

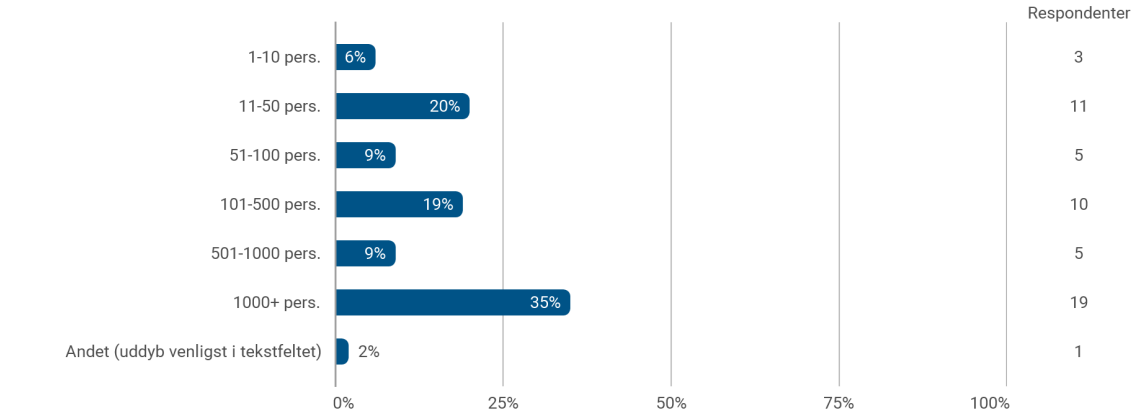


[23] Kommentarer fra tekstfelt Andet sted: "Fælleskommunal indkøbsorganisation, selvejende virksomhed vedtaget ved lov, Interesse varetagelses organisation"

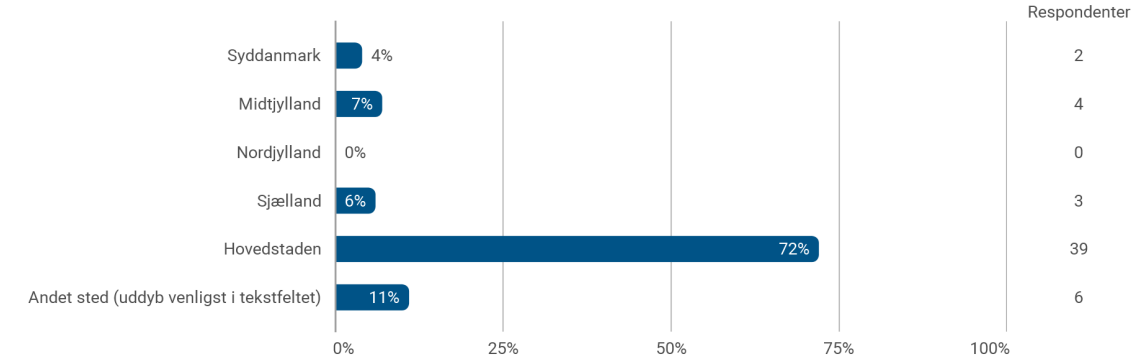
Hvilken sektor arbejder du i?[24]



Hvor mange medarbejdere har din organisation?[25]



I hvilken region ligger din arbejdsplads?[26]



Opsummerende har surveyens respondentliste en meget høj forekomst af personer med ledelsesansvar, der er særligt kvalificerede til at vurdere aftagerbehov, da de for en stor dels

[24] Kommentarer fra tekstfelt Anden sektor: ”Teknologi, Konsulentbranchen, It sikkerhed, Erhvervssektoren, Sikkerhedsbranchen, It-sikkerhedskonsulent- og softwarehus, Consumer manifacturing, Interesseorganisation, Erhvervsdrivende fond, IT-"sektoren", IT software, politisk organisation, Life Science, IT & Teknologi, fond, Erhvervsorganisation, Forsyning, Detail, Kommunale, Forsvar og rumfart, Uddannelses- og Forkningssektoren [fjernet for at sikre anonymitet], x, Finansministeriet, Public Affairs i faglig akademisk organisation, IT-rekruttering, Leverandør af cybersikkerhedsydelser, Cyber Security / Soft and Hardware”

[25] Kommentarer fra tekstfelt Andet: ”80000”

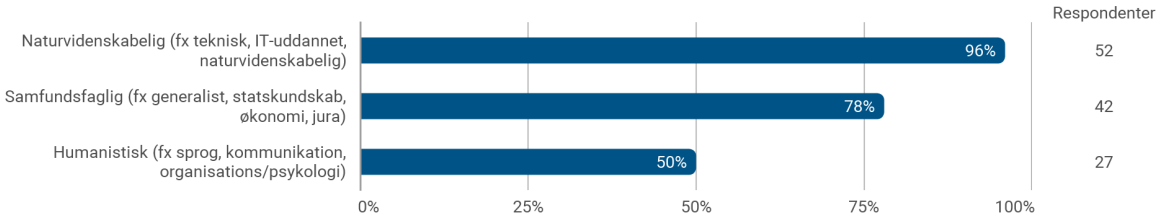
[26] Kommentarer fra tekstfelt Andet sted: ”Har hovedkontor i DK, men har mere end 1400 faciliteter fordelte i 80+ lande, hele danmark, vi har kontorer flere steder, men min arbejdsplads er i KBH, I hele Danmark, Globalt med hovedsæde i Østjylland, Hele Norden”

vedkommende må antages at deltage i rekrutteringsprocesser. Respondenterne er hovedsageligt ansatte i den private sektor (70%) og i mindre grad staten (22%), hele 35% arbejder i organisationer med over 1000 personer og arbejdspladsen er for 72% placeret i hovedstadsregionen. Disse karakteristika flugter i høj grad med vurderingerne fra den kvalitative behovsanalyse i forhold til hvilke type aftagere, MICS er relevant for (se næste afsnit).

9. Relevans af MICS og estimat over antal potentielle studerende

Overordnet har respondenterne fra de kvalitative interviews givet udtryk for, at der findes et klart behov for MICS-uddannelsens fokus og kompetencer. Det samfundsvidenskabeligt analytiske sigte koblet med praksisnære færdigheder indenfor både cyber og intelligence bliver set som et efterspurgt kompetenceløft for en bred personalegruppe, der ifølge respondenterne spænder fra IT-afdelingens teknikorienterede personale, der har brug for en samfundsfaglig vinkel, over et bredt ledelseslag og helt op til topledelsen og ledelsesrådgivning. Surveyen har fulgt op på dette ved at undersøge respondenternes vurdering af, hvem MICS vil være relevant for. Fra de kvalitative interviews vurderes det, at MICS-uddannelsen især henvender sig til større organisationer, virksomheder i international konkurrence og det stigende antal myndigheder samt private aktører, der regulatorisk skal indgå i samarbejder med de statslige efterretningstjenester.

Hvilken uddannelsesmæssig baggrund vil MICS være relevant for? (vælg gerne flere)

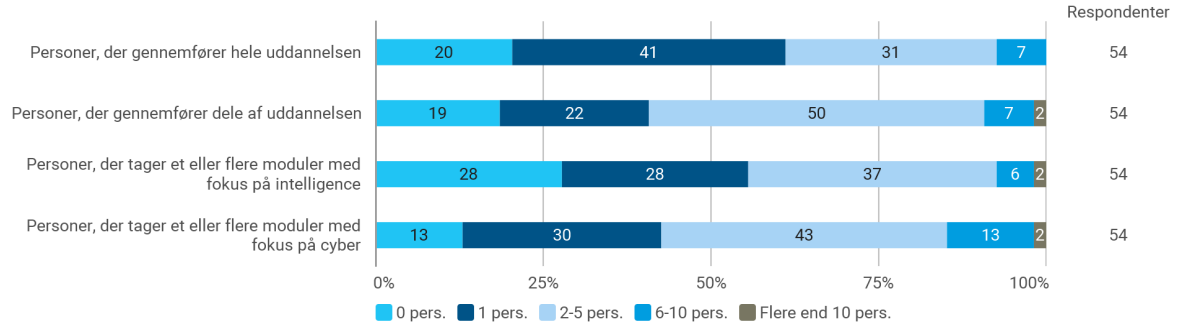


Angiv gerne særlige uddannelser eller stillingsbetegnelser, som MICS vil være relevant for:

> ”CIO; risk manager; Kendskab til sikkerhedsrådgivningsfirmaer; Chief Risk Officer; Ansøgere med arbejdserfaring indenfor området; Uddannelsesparathed skal selvfølgelig være tilstede, men en videreudvikling af eksisterende sikkerhedsfolk med f.eks. en forsvarsbaggrund e.lign. bør også eksistere; Vi har behov for at løfte niveauet, ikke udskifte en erfaren organisation; alle; Security risk management, Københavns Universitet; Bsc i it-sikkerhed, Ingeniører, datamatikere.”

Der kan konstateres en stor åbenhed overfor, at MICS kan være relevant for medarbejdere fra vidt forskellige baggrunde (humaniora får uventet høj opbakning) og at praktisk talt alle respondenter angiver, at personer med en teknisk baggrund kan drage fordel af uddannelsens samfundsvidenskabelige sigte. (Top)ledelsesperspektivet bemærkes igen og flugter således, som tidligere nævnt, med ledelsesforankringen i den næste cyber- og informationssikkerhedsstrategi.

Hvor mange personer vurderer du, at MICS kan være relevant for i din organisation over de næste fem år?



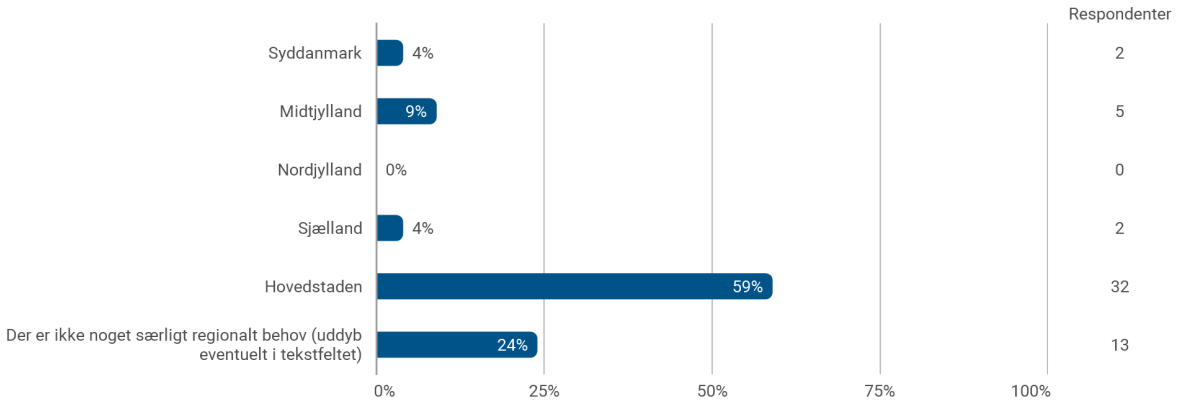
Den elektroniske survey uddyber det generelt konstaterede behov for MICS, når respondenterne vurderer antallet af potentielle studerende som deres organisation kan levere i den nærmeste fremtid. Det er især interessant, at kun 20% ikke mener, at gennemførelse af en fuld MICS kunne være relevant for nogen i deres organisationen, mens 80% mener, at det kunne være relevant og hele 7% peger på en tilgang på 6-10 personer. Der er dog naturligvis begrænsninger i disse tilkendegivelser og i formuleringen af spørgsmålet, men resultatet er selv med en konservativ tilgang positivt.

Behovsanalysen udgør ikke et sikkert fundament for at vurdere antallet af potentielle MICS-studerende fra spor 2, offentlig-privat sikkerhedsspor. Et estimat baseret på de foreliggende tal kunne dog være 2-5 fuldtidsstuderende og 6-10 studerende, der tager et eller flere moduler, men der må tilskrives disse tal stor usikkerhed.

9.1. Nationalt og regionalt behov for MICS

De kvalitative interviews har alle peget på cybertrusler som grænseoverskridende og dermed ikke geografisk betinget. Dog er der en naturlig fortættet tilstedeværelse af store organisationer i hovedstadsområdet, der i højere grad end mindre organisationer vil have ressourcer og incitament til at benytte MICS-uddannelsen. Dette ses også i resultaterne fra surveyen.[27]

I hvilken region vil du vurdere behovet for MICS-uddannelsen er størst over de næste fem år?



Der er ikke noget særligt regionalt behov (uddyb eventuelt i tekstfeltet):

> ”der er store danske virksomheder på begge sider af storebælt; ved jeg ikke noget om; Cyber er vigtigt i hele landet; Mener det er styret af organisationernes placering, ikke af den enkelte region.; 100% virtuelt som alt indholdet bør være, alternativt i hovedstaden hvor 99% af arbejdet efterfølgende er; samme problem i hele landet; Der vil være behov ift. alle regioner;

[27] Der kan antages en vis bias i besvarelsen, da 72% af respondenterne arbejder i hovedstadsområdet.

Hovedstaden, Midtjylland og Syddanmark; Behov generelt i alle dele af landet; xxx; Behovet for MICS-uddannelsen er relevant for hele Danmark; Vi ser mere og mere fjernarbejde der udvisker regionale grænser. Samtidig er der ingen grund til at tro cyber kriminelle og politiske interessenter kigger på postnummer når de vælger en strategi."

MICS-uddannelsen vil hovedsageligt foregå online, men indebærer også en række fysiske aktiviteter og planlagt tilstedeværelse, der foregår enten på SDU, i Forsvarsakademiets lokaler på Frederiksberg Slot samt på internat tæt på hovedstadsområdet. Placeringen af undervisningen på MICS henholdsvis online og med fysisk tilstedeværelse er således i overensstemmelse med de udtrykte behovsvurderinger angående fleksibilitet samt behov for netværksdannelse.

9.2. Match mellem MICS og behovsanalysen: Fagligt indhold og uddannelsens tilrettelæggelse

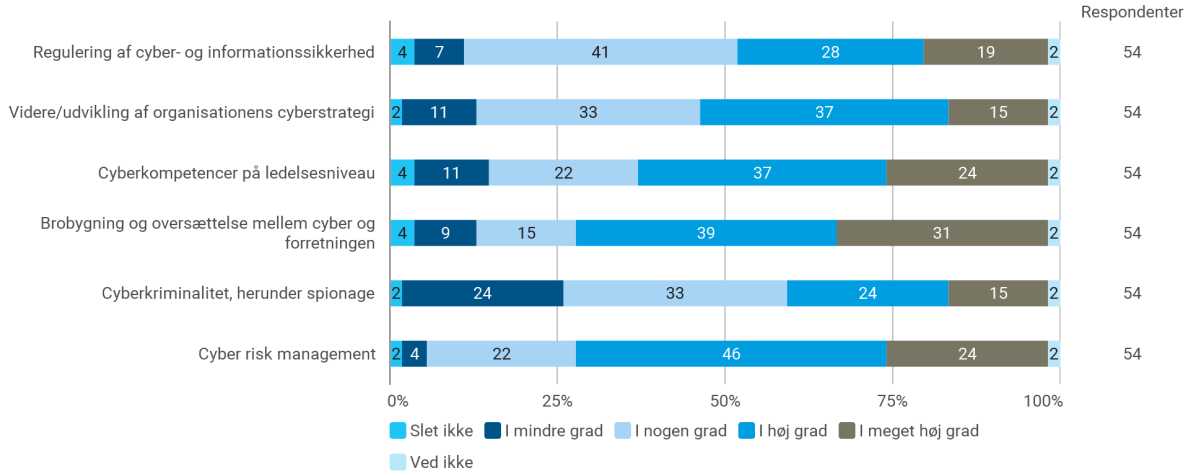
Ovenstående behovsanalyse af MICS har konstateret både efterspørgsel og relevans. Relevansen skal fremstå tydeligt for aftagerne, der ser MICS som både en økonomisk investering, et træk på medarbejderens arbejdstid og opkvalificering af organisationen. Der kræves derfor en vis grad af kontinuerlig tilpasning, især i lyset af hastigt skiftende trusselsbilleder. Behovsanalysen har af den grund eksplicit undersøgt efterspørgslen på forskellige dele af MICS' fagelementer.

I løbet af de kvalitative interview opstod der en række "mættede vurderinger" på områder, hvor der blandt respondenterne var en forholdsvis høj grad af enighed. Disse præsenteres i det følgende sammen med surveyens resultater.

- **Oversætteren:** Et generelt ønske til MICS-kandidaterne er, at de kan indtage den meget efterspurgte rolle som "oversætter" eller "brobygger" mellem det tekniske niveau og resten af organisationen. Organisationens mellemlederlag skal kunne forstå og formidle trusler, risikovurderinger, prioritere initiativer og tænke strategisk i forhold til at identificere og udbedre sårbarheder på tværs. Respondenterne ser et helt konkret behov for den tværfaglige, ikke-tekniske kompetenceopbygning i MICS og bemærker, at dette flugter med generelle krav om digital opkvalificering på cyber- og informationssikkerhed.

Surveyen viser også tydeligt, at organisatorisk og kommunikativ brobygning er en klar prioritering på linje med cyberrisk management og cyberkompetencer hos ledelsen.

I hvilken grad har din organisation behov for at tilføre kompetencer på nedenstående cyber-områder indenfor de næste fem år?[28]



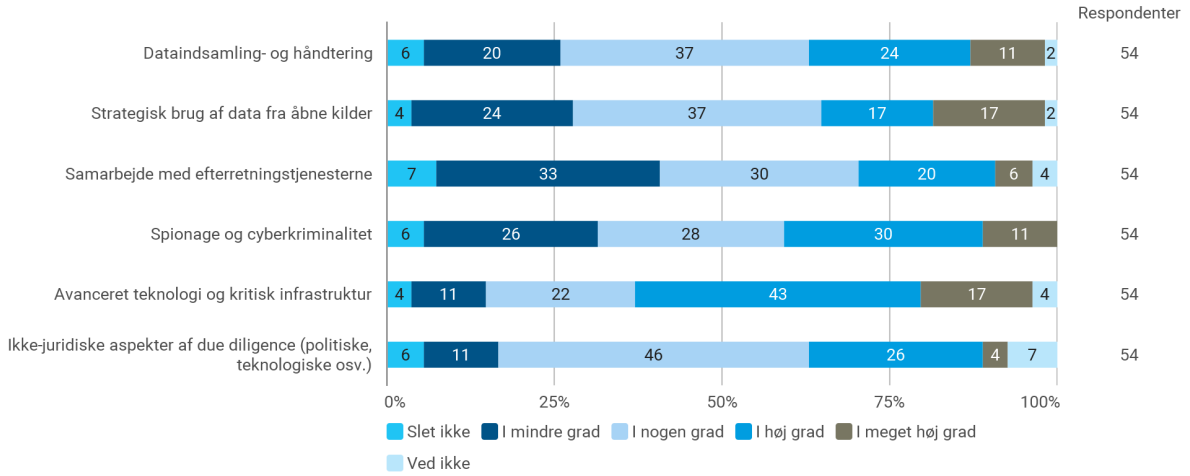
- **Match til oversætteren:** Disse ønsker efterkommes helt praktisk gennem eksempelvis Foresight analysis-workshoppen på andet semester og Simulation Intelligence Analysis Exercise på tredje semester, der begge bringer foregående moduler sammen ved at placere den studerende i rollen som den efterspurgte "brobyggende oversætter". Den store efterspørgsel på disse specifikke punkter vil også påvirke udformningen af aktiviteterne, så ledelsesbriefing, beslutnings- og kommunikationsprocesser opprioriteres. Uddannelsens juridiske fagelementer taler direkte ind i de regulatoriske behov, mens MICS' cyberspor gennem militærstrategisk analyse leverer på de efterspurgte cyberstrategiske aspekter.

En gennemgående bemærkning fra de kvalitative interviews angår intelligence-delen af MICS, hvor det vurderes at danske aktører ofte kun er perifert bekendte med indhold, metoder og (forretnings)muligheder i efterretningsanalyse og -praksisser.

- **Opdyrk intelligence-markedet:** En vis forbeholdenhed overfor intelligence som ord/koncept kan spores hos de kvalitative respondenter, der i kraft af deres egen baggrund i mange tilfælde selv har erfaring med efterretningsarbejde. De fortæller, at markedet for intelligence skal modnes hos aftagerne. Surveyen konstaterer også en relativt mindre interesse i intelligence i forhold til cybersporet, men resultatet nuancerer dog den forbeholdne holdning, når eksempelvis 34% svarer "I meget høj grad" eller "I høj grad" til organisationens behov for at tilføre kompetencer på strategisk brug af data fra åbne kilder. Hele 60% kan med de samme svarkategorier genkende et behov for at tilføre intelligence-kompetencer på avanceret teknologi og infrastruktur over de næste fem år.

[28] *Angiv gerne andre cyber-kompetencer i tekstfeltet*: "Tekniske fagligheder relateret til infosec; har oplevet ransomware... ingen yderligere "kompetancer" ud over hard core teknik til at reducere risici; Cyberanalytiker (tekniker); Cost module - investment in cs versus risks; Information Security Management, SOC; Kompetencer på formidlingsområdet, herunder ift. ekstern rådgivning og kompetenceopbygning. Tekniske kompetencer indenfor OT sikkerhed; Nu kender jeg selv meget til området, så behovene er der selvfølgelig åbenlyst i min organisation, men om de er identificeret hos dem, der arbejder med området, ved jeg ikke. Jeg arbejder ikke selv med cybersec her; Svar baseret på det vi forventer vores kunder efterspørger."

I hvilken grad har din organisation behov for at tilføre kompetencer på nedenstående intelligence-områder indenfor de næste fem år?[29]



- **Match til "opdyrk intelligence-markedet":** Der vil blive gjort en særlig målrettet indsats for at tydeliggøre anvendeligheden af intelligence-sporet overfor aftagerne i behovsanalysens offentlig-private sikkerhedsspor. Aftagerne hos FE, PET og Forsvaret har helt umiddelbare behov for efterretningskompetencer.

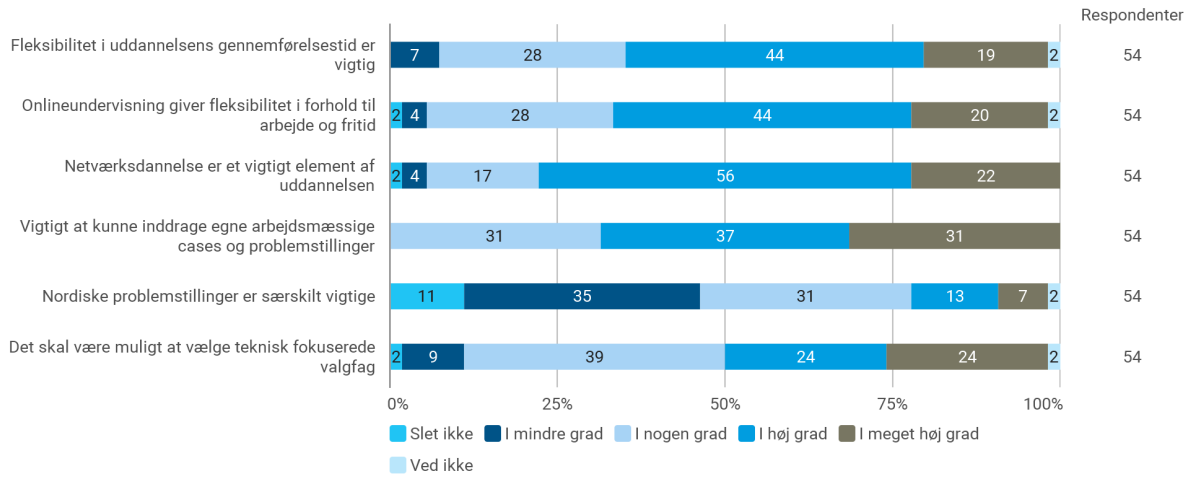
Både aftagere fra spor 1, forsvars- og politimyndigheder, og spor 2, offentlig-privat sikkerhedsspor, har klare forventninger om en anvendelsesorienteret uddannelse, der højner den studerendes analytiske kapacitet både teoretisk og praktisk. Deraf følger en mættet vurdering om nytten af praktiske værktøjer.

- **Praksis:** MICS skal give mening for aftageren og den studerende gennem praktisk anvendelighed, hvilket får respondenterne til at stille krav om en balanceret afvejning af teori og praksis. Det er tydeligt, at respondenterne skelner skarpt mellem en kandidatuddannelse og en professionel master målrettet erhvervsaktive personer. Der stilles ikke i samme grad praktiske krav til en kandidatuddannelse som til en master, hvor antagelsen er, at organisationen kan se konkrete forbedringer som resultat af forløbet.

Surveyen understreger denne pointe gennem kategorien om, hvorvidt det er vigtigt at kunne inddrage egne arbejdsmæssige cases og problemstillinger. Hele 31% af respondenterne svarer "i meget høj grad" og ingen svarer "I mindre grad" eller "Slet ikke".

[29] *Angiv gerne andre intelligence-kompetencer i tekstfeltet*: "Tror man skal være offentlig ansat for at undgå økonomiske realiteter; Structured Intelligence analysis with the intel process; Threat analyse; Svar baseret på hvad vi forventer at vores kunder efterspørger; Synes at der generelt i DK er et regulatorisk problem i at Cybersikkerhed nærmest er ud deligeret til de virksomheder der er en del af den kritiske infrastruktur."

I hvilken grad er du enig i nedenstående udsagn om MICS som en professionel master uddannelse?[30]



- **Match til praksis:** Udover Foresight Analysis workshop og Simulation Intelligence Analysis Excercise, så prioriteres inddragelse af cases, current events, og sammenhæng i undervisningen til analyser af egne problemstillinger fra organisationen. Det sker gennem invitation af gæsteforelæsere med praktisk indsigt i de to emner samt mulighed for at skrive eksamensopgaver, Certifikat projekt og master-projekt under inddragelse af selvvalgt litteratur og problemformuleringer fra egen jobsituation. Derudover arbejder både intelligence- og cybersporet målrettet henimod kulminerende praktiske flerdages scenarieanalyser med fysisk tilstedeværelse.

I forlængelse af praksis-forventningen ligger forventningen om netværksdannelse, der er en særlig professionel kvalifikation i sig selv og som kan være afgørende i krisesituationer.

- **Netværk:** Netværksdannelse bliver i de kvalitative interviews fremhævet som et eftertragtet element i MICS-uddannelsen og der argumenteres for afgrænset, men prioriteret fysisk tilstedeværelse. Hele 78% svarer i surveyen enten "I meget høj grad" eller "I høj grad" til at netværksdannelsen er et vigtigt element af uddannelsen. De kvalitative respondenter giver udtryk for, at fysisk fremmøde i starten af uddannelsen vil være faciliterende for samarbejde og fortrolighed – også i forbindelse med den efterfølgende online undervisning. Muligheden for at skabe kontakter mellem efterretningstjenesterne og de civile aktører anses som et værdifuldt gode såfremt personligt møde har fundet sted forudgående.

- **Match til netværk:** MICS prioriterer fysiske opstartsaktiviteter hvert semester, dannelse af studiegrupper og didaktiske, studenterdrevne undervisningsaktiviteter, der har til formål at skabe et læringsfællesskab. Derudover vil de koncentrerede praktiske øvelser, der finder sted over en eller flere sammenhængende dage bidrage til netværksdannelse og der etableres et alumnenetværk.

I forhold til uddannelsens opbygning har der dannet sig en mættet vurdering angående undervisningsformat og fleksibilitet, der har stor betydning for erhvervsaktive studerende.

[30] *Angiv gerne andre ønsker til uddannelsen i tekstfeltet*: "onlineundervisning risikere at mindske kvaliteten af undervisningen; Dybt bekymrende at udd. tilsyneladende er u-teknisk og ikke udbudt internationalt; Uddannelse på engelsk; Udarbejde Risikovurderinger; Fokus på krydsfeltet mellem policyudvikling og efterretning er vigtigt, ikke mindst ift. spørgsmål om demokratisk kontrol når efterretning bliver en del af politik- og strategiudvikling; Forretningsforståelse er essentiel; Samfundsmæssige aspekter af at DK er højt digitaliseret men at vi sikkerhedsmæssigt nok er bagud."

- **Undervisningsformatet og fleksibilitet:** Et klart flertal af respondenterne er positivt indstillede overfor onlineundervisning og ser det som ønskeligt, da det giver både den studerende og dennes arbejdsplads fleksibilitet. Asynkron undervisning med optagede videoer bemærkes som en særlig fordel for virksomheder med ansatte i flere forskellige tidszoner. Kun 2% af surveyens respondenter er afvisende overfor onlineundervisning.

- **Match til undervisningsformatet og fleksibilitet:** MICS udbydes primært som en online master, hvor asynkrone undervisningsaktiviteter bevidst inddrages for at understøtte uddannelsens pædagogiske aktionslæringsprincipper, der givet fleksibiliteten blandt andet højner muligheden for at arbejde med egne cases og problemstillinger. Desuden efterkommes den overvældende præference om fleksibilitet i forhold til uddannelsens gennemførelsestid ved at gennemførelsestiden kan strækkes fra 2 til 4 år i alt.

Uddannelsens unikke samfundsvidenskabelige karakter fremgår af behovsanalysens sammenligning med tilnærmende uddannelser på det danske marked, der gør det klart, at der er en betydelig distance fra MICS til de teknisk fokuserede cybersikkerhedsuddannelser. Og da feltet fundamentalt set er meget teknisk, har de kvalitative respondenter også udtrykt ønsker i retning af muligheden for tekniske valgfag og surveyen viser ligeledes, at 48% af respondenterne ønsker dette "I meget høj grad" eller "I høj grad".

- **Tekniske valgfag:** Aftagerne har også et fokus på helt praktiske og umiddelbart anvendelige kompetencer, såsom eksempelvis brug af særlig software. Disse udbud findes i overvejende grad allerede på markedet i dag og selvom efterspørgslen er forståelig, så vurderes det ikke som en umiddelbar oplagt vej at gå i opstarten af MICS, givet uddannelsens særlige samfundsvidenskabelige karakter.

- **Match til tekniske valgfag:** Der er foretaget en afsøgning af MICS-kompatible tekniske valgfag, der også tager højde for, at en stor del af de studerende ikke har en teknisk uddannelsesbaggrund. Denne forudsætning indsnævrer feltet af tekniske valgfag voldsomt og der er ikke fundet passende udbud for nuværende. MICS vil fremadrettet være opmærksom på efterspørgslen og tage denne under overvejelse i forhold til nye valgfag.

10. Behov for sprogligt udbud af MICS på engelsk

De kvalitative interviews har afdækket en udtalt bekymring for manglen på kvalificeret arbejdskraft indenfor IT-branchen som helhed samt et særligt fokus på hvordan organisationers cybersikkerhed lider under denne udfordring og i stigende grad har brug for at IT-medarbejdere også har samfundsfaglige/sikkerhedspolitiske kompetencer. Problemstillingen forsøges afhjulpet gennem en stigning i ansættelser af udenlandske medarbejdere og på den baggrund er der blandt de interviewede stor enighed om, at MICS-uddannelsens sprog optimalt set bør være engelsk. Især indenfor det offentlig-private sikkerhedsspor er der en forventning om, at MICS tager arbejdskraftsmanglens sproglige behov til efterretning og derigennem letter adgangen for private virksomheder. Der er forståelse for, at der på forsvars- og politisporet er behov for et Nordisk/dansk perspektiv og dansksprogede elementer, men det pointeres bredt, at sprognormen indenfor informations- og cybersikkerhed helt generelt er engelsk.

Påpegningen af behovet for en engelsksproget MICS førte til en yderligere undersøgelse af de større strukturelle behov. De nedenstående, omfattende undersøgelser lægges til grund for beslutningen om at udbyde MICS på både dansk og engelsk.

Cybersikkerhedsbranchen havde i 2020 et globalt arbejdskraftsunderskud på 3,1 millioner ubesatte stillinger, hvoraf de cirka 168.000 var i Europa.[31] Denne problemstilling har naturligvis også store konsekvenser i Danmark. Ifølge IT-Branchen har 45,2% af danske it-virksomheder opgivet af besætte stillinger grundet arbejdskraftsmangel og hver tredje virksomhed har følgeligt måtte afvise ordrer og opgaver.[32] Alene i andet halvår af 2019 blev rekrutteringen af kvalificerede medarbejdere til 2000 digitale specialiststillinger opgivet, men alligevel blev 1150 af disse besat af en profil, der manglede væsentlige kvalifikationer og 850 forblev ubesatte.[33] Og til trods for at antallet af udenlandske it-specialister i danske stillinger er steget med 48% mellem 2016-2019, er der således stadig udækkede behov.[34] Et særligt problematisk aspekt af denne arbejdskraftsmangel viser sig gennem, at virksomheder overser cybertrusler ved bevidst at ignorere disse, undlade at efterforske dem og ultimativt ikke formår at løse it-sikkerhedshændelser.[35]

I Danmark er efterspørgslen efter informationssikkerhedskompetencer (cyber- og it-sikkerhed) tredoblet mellem 2008 og 2018, hvor henholdsvis 1.700 og 5.000 stillingsopslag efterspurgte disse kompetencer og dermed overstiger de den samlede stigning i efterspørgsel efter arbejdskraft.[36] Forventningen er at disse rekrutteringsudfordringer intensiveres i årene frem mod 2030 og at 13.000 nye informationssikkerhedsstillinger skal besættes.[37]

Denne hårde konkurrence om kvalificerede medarbejdere resulterer i stor arbejdskraftsmobilitet over landegrænser, hvilket fremmer en øget brug af engelsk i arbejdssituationer. Behovet for rekruttering af engelsktalende udenlandske medarbejdere vil således være stigende og i tiltrækningen af disse vil mulighederne for en efteruddannelse som MICS på engelsk både være en oplagt konkurrenceparameter samt en mulighed for opkvalificering efter ansættelse. Flere respondenter gør opmærksom på, at sproget indenfor kurser i cybersikkerhed naturligt er engelsk qua feltets geografiske grænseløshed, at den faglige værktøjskasse indenfor feltet er mættet af engelske ord og koncepter samt at arbejdssproget i stigende grad er engelsk i større danske organisationer. Alle i 2016 konstaterede en undersøgelse fra Dansk Industri, at koncernsproget er engelsk i cirka 75% af alle danske virksomheder med flere end 100 ansatte.[38] En engelsksproget MICS er også blevet anført som en fordel i eksempelvis at gøre det fælleseuropæiske samarbejde gennem EU's European Network and Information Security Agency (ENISA) mere frugtbart. Overordnet set vil et engelsksproget udbud af MICS i tilgift til den danske medvirke til at nedbryde sproglige barrierer, der ellers kan opstå i daglige samarbejder. Der gøres ligeledes opmærksom på, at en fuldt engelsksproget uddannelse er attraktiv

[31] (ISC)² (2020): *Cybersecurity Workforce Study 2020*, s. 16-17 https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx
[32] IT-Branchen (2019): Danmark taber den digitale fødekæde https://itb.dk/maerkesager/kapital-til-vaekst/danmark-mister-den-digitale-foedekaede/
[33] Digital Dogme (2020): *Det digitale kompetencebarometer 2020*, s. 11 https://download.digitaldogme.dk/hubfs/Det%20digitale%20Kompetencebarometer%202020.pdf
[34] PROSA (2020): *Vækst i udenlandsk it-arbejdskraft, mens dansk it-ledighed stiger* https://via.ritzau.dk/pressemeddelelse/vaekst-i-udenlandsk-it-arbejdskraft-mens-dansk-it-ledighed-stiger?publisherId=13559092&releaseId=13600202
[35] Version2 (2020): *Advarsel om mangel på it-sikkerhedsfagfolk: Sikkerhedsalarmer må ignoreres* https://www.version2.dk/artikel/advarsel-mangel-paa-it-sikkerhedsfagfolk-sikkerhedsalarmer-maa-ignoreres-1087968
[36] Højbjerre Brauer Schultz (2019): *Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark*, s. 9 https://erhvervsstyrelsen.dk/sites/default/files/2020-03/Arbejdsmarkedet%20for%20informationssikkerhedskompetencer%20i%20Danmark%20-%20Rapport.pdf
[37] Højbjerre Brauer Schultz (2019): *Arbejdsmarkedet for informationssikkerhedskompetencer i Danmark*, s. 6 https://erhvervsstyrelsen.dk/sites/default/files/2020-03/Arbejdsmarkedet%20for%20informationssikkerhedskompetencer%20i%20Danmark%20-%20Rapport.pdf
[38] Ingeniøren (2016): *Du kommer ikke udenom at blive bedre til engelsk. Flere danske virksomheder får engelsk som koncernsprog* https://ing.dk/artikel/du-kommer-ikke-udenom-at-blive-bedre-engelsk-flere-danske-virksomheder-faar-engelsk

for en bredere kreds af potentielle aftagere udenfor Danmark, hvilket kunne tilføre uddannelsen et eftertragtet internationalt netværk.

Det engelsksproglige behov understreges af, at it-ansatte til danske stillinger i de senere år især er rekrutteret fra Indien, Rumænien, Litauen og Bulgarien[39] og at disse ansatte ikke kan forventes at leve op til sprogkrav for en dansk masteruddannelse, eftersom deres ophold ikke betinges af gennemførelse af danske sprogkurser, da de enten er EU-borgere eller som tredjelandsborgere bliver ansat på baggrund af beløbsordningen eller positivlisten.

Det engelske sprogønske efterkommes ved, at en andel af fagelementerne også kan tilgås for engelsksprogede og at en engelsksproget version af MICS med alternative kurser på andet semester søges prækvalificeret parallelt med en dansksproget version af uddannelsen. I praksis vil de to uddannelser i forbindelse med fælles fag samundervises indenfor ét enkelt læringsfællesskab, hvor nogle deltagere er indskrevne på den dansksprogede version, mens andre vil være indskrevne på den engelsksprogede version og hvor alle har fleksibilitet i forhold til specialisering, varighed og deres individuelle erhvervsorientering.

Opkvalificering af udenlandske arbejdstagere gennem en engelsksproget MICS vil således bidrage til at opfylde meget konkrete arbejdsmarkedsbehov, der ikke i tilstrækkeligt omfang kan opfyldes af en dansksproget MICS-uddannelse. Det er en central del af MICS-uddannelsens formål at højne det danske samfunds cybersikkerhedsniveau og det kræver, at uddannelsen også bliver udbudt på engelsk.

11.Konklusion på behovsanalysen

De ovenstående analyser viser behov for og efterspørgsel efter MICS på både nationalt og regionalt plan samt i de kritiske sektorer. Dertil kommer at MICS-uddannelsen har konkrete tilkendegivelser fra uddannelsens start fra forsvars- og politimyndigheder for 13-15 studerende og mindst 6-7 studerende på enkeltmoduler. Behovsanalysen med aftagere i flere sektorer indenfor det offentlige-private giver desuden en forventning om et mindre antal fuldtidsstuderende (2-5 fra de adspurgte) samt et større antal (6-10) enkeltmodulsstuderende. Der er derfor et godt grundlag for at starte MICS-uddannelsen indenfor de økonomiske rammer, der er opstillet, og der er god grund til at forvente et stigende antal studerende efterhånden som behovet for viden og kompetencer på cyber- og intelligence områderne stiger og uddannelsen bliver mere kendt ude i samfundet.

Udviklingen af MICS-uddannelsen er baseret på dialog mellem FAK og SDU samt dialog med centrale aktører i de to identificerede spor: spor 1, forsvars- og politimyndigheder samt spor 2, offentlig-privat sikkerhedsspor. De udtrykte behov har i høj grad formet udviklingen af MICS og sikret et godt match mellem udbud og efterspørgsel på både fagligt indhold og uddannelsens praktiske tilrettelæggelse. I særlig grad har behovsanalysen informeret valget om at udbyde MICS på både dansk og engelsk. En sådan dialog vil fortsætte, blandt andet gennem oprettelse af et aftagerpanel med deltagere fra begge spor, for at sikre at uddannelsen forbliver samfundsrelevant og attraktiv for aftagere – også selvom de to emneområder må antages at udvikle sig betydeligt over de kommende år.

[39] Computerworld (2020): *Det vælter ind i Danmark med udenlandske it-folk - men der er stadig ikke nok* https://www.computerworld.dk/art/253412/det-vaelter-ind-i-danmark-med-udenlandske-it-folk-men-der-er-stadig-ikke-nok

Uddannelses- og Forskningsstyrelsen

Syddansk Universitet
E-mail: sdu@sdu.dk

Godkendelse af ny uddannelse

Uddannelses- og forskningsministeren har på baggrund af gennemført prækvalifikation af Syddansk Universitets (SDU) ansøgning om godkendelse af ny uddannelse truffet følgende afgørelse:

Godkendelse af masteruddannelse i Intelligence og cyber studier

12. april 2021

Uddannelses- og Forskningsstyrelsen
Uddannelsesudbud og Optag

Haraldsgade 53
2100 København Ø
Tel. 7231 7800

www.ufm.dk

CVR-nr. 3404 2012

Ref.-nr.
20/49052-1

Afgørelsen er truffet i medfør af § 20 i bekendtgørelse nr. 853 af 12. august 2019 om akkreditering af videregående uddannelsesinstitutioner og godkendelse af videregående uddannelser.

Det er en forudsætning for godkendelsen, at uddannelsen og dennes studieordning skal opfylde uddannelsesreglerne, herunder bekendtgørelse nr. 19 af 9. januar 2020 om masteruddannelser ved universiteterne (masterbekendtgørelsen) og bekendtgørelse nr. 24 af 9. januar 2020 om deltidsuddannelser ved universiteterne (deltidsbekendtgørelsen) med senere ændringer.

Da SDU er positivt institutionsakkrediteret gives godkendelsen til umiddelbar oprettelse af uddannelsen.

Ansøgningen er blevet vurderet af Det rådgivende udvalg for vurdering af udbud af videregående uddannelser (RUVU). Vurderingen er vedlagt som bilag.

Hovedområde:
Uddannelsen hører under det samfundsvidenskabelige hovedområde.

Titel:
Efter reglerne i masterbekendtgørelsens § 5 fastlægges uddannelsens titel til:

Dansk: Master i intelligence og cyber studier

Engelsk: Master of Intelligence and Cyber Studies

Udbudssted:
Uddannelsen udbydes i Odense

Sprog:
Ministeriet har noteret sig, at uddannelsen udbydes på dansk.

Normeret studietid:
Efter reglerne i masterbekendtgørelsens § 6, stk. 2, fastlægges uddannelsens normering til 60 ECTS-point.

Takstindplacering:
Uddannelsen indplaceres til: Takst 1 (deltid)
Aktivitetsgruppekode: 5959

Koder Danmarks Statistik:
UDD: 8584
AUDD: 8584

Censorkorps:
Ministeriet har noteret sig, at uddannelsen tilknyttes Censorkorpset for Statskundskab med supplering fra Forsvarsakademiets Censorkorps for Forsvarets akkrediterede uddannelser]

Uddannelses- og Forskningsstyrelsen

Adgangskrav:
Efter det oplyste er følgende uddannelser adgangsgivende til masteruddannelsen, jf. § 9, i bekendtgørelse nr. 19 af 9.januar 2020 i masterbekendtgørelsen:

Ansøgere til MICS skal have gennemført en relevant uddannelse inden for det samfundsvidenskabelige, naturvidenskabelige eller humanistiske felt på enten professionsbachelor-, bachelor- eller kandidatniveau. Nedenstående er eksempler på videregående uddannelser, der giver adgang til optagelse på MICS, under forudsætning af relevant erhvervserfaring:

- Professionsbacheloruddannelse inden for offentlig administration, IT, diplomingeniør, kommunikation, sikkerhed, strategi og økonomi.

- Bachelor eller kandidatuddannelse inden for statskundskab, jura, psykologi, sprog, økonomi, fysik, matematik, datalogi og Softwareudvikling.

For ansatte i Forsvaret er kravet at være officer under Forsvarsministeriets myndighedsområde – herunder også Beredskabsstyrelsen – på M321/U321 eller M322/U322 niveau.

Ansøgere til MICS skal som minimum have to års relevant erhvervserfaring efter at have gennemført den adgangsgivende uddannelse. Relevant erhvervserfaring kan udgøres af, at ansøgeren enten tidligere eller for nuværende beskæftiger sig med analyse, ledelse, efterretninger, informationssikkerhed, risikohåndtering, forsyningssikkerhed, forretningsudvikling og formidlingsaktiviteter.

Der kan søges om dispensation for ansøgere, der opfylder kravet om minimum to års relevant erhvervserfaring, men ikke opfylder uddannelseskravet.

Ansøgere skal kunne dokumentere deres engelskkundskaber i henhold til SDUs gældende sprogkrav https://www.sdu.dk/da/uddannelse/kandidat/adgangskrav/sprogkrav.

Studerende, der ikke ønsker at deltage i alle studiets elementer, kan optages som enkeltfagsstuderende, hvis forudsætningerne i henhold til adgang (se ovenfor) er

opfyldte; hvis adgangskravene til det pågældende enkeltfag er opfyldt af den studerende, og hvis universitetet finder optagelsen hensigtsmæssig ud fra praktiske og pædagogiske hensyn. Grundfag I, From Cold War Espionage to Cyberwars: history, theory, and practice of intelligence and cybersecurity er obligatorisk for alle studerende. På grund af den faglige progression forventes den enkeltfagsstuderende at have tilegnet sig de samme faglige forudsætninger som den almindelige studerende.
Der udstedes bevis for beståede fag, og der kan udstedes et Certifikatbevis for den studerende, der har gennemført mindst 30 ECTS og har skrevet et bestået Certifikatprojekt (5ECTS), det vil sige i alt 35 ECTS.

Med venlig hilsen

Camilla Badse

Specialkonsulent

Uddannelses- og Forskningsstyrelsen

Nr. A5 - Ny uddannelse – prækvalifikation (forår 2021)			**Status på ansøgningen:** Under behandling	
Ansøger og udbudssted:	SDU, Campus Odense			
Uddannelsestype:	Master			
Uddannelsens navn (fagbetegnelse):	Intelligence og cyber studier			
Den uddannedes titler på hhv. da/eng:	Dansk: Master i intelligence og cyber studier Engelsk: Master of Intelligence and Cyber Studies			
Hovedområde:	Samfundsvidenskab		**Genansøgning:** *(ja/nej)*	Nej
Sprog:	Dansk	**Antal ECTS:**	60 ECTS	
Link til ansøgning på http://pkf.ufm.dk:	http://pkf.ufm.dk/flows/83fc54461ecd40b8cce1caf593041b79			
RUVU's vurdering	RUVU vurderer, at ansøgningen opfylder kriterierne som fastsat i bekendtgørelse nr. 853 af 12. august 2019, bilag 4. RUVU vurderer, at uddannelsen kan imødekomme et behov for et generelt løft af ikke-tekniske kompetencer inden for intelligence og cyber-sikkerhed hos beslutningstagere, myndigheder og erhvervsliv. RUVU har noteret sig, at hovedparten af uddannelsen tilrettelægges online. RUVU lægger desuden til grund for sin vurdering, at behovet for uddannelsen afspejles af Forsvarsakademiets engagement i både udviklingen og gennemførelsen af uddannelsen. RUVU er skeptisk i forhold til, om der er behov for både en dansksproget og en engelsksproget masteruddannelse i Intelligence og cyber studier, og mener, at SDU indledningsvis kun bør åbne den ene af de to uddannelser og derefter lade efterspørgslen hos kursisterne afgøre behovet for at åbne begge.			