digitaliserings og ligestillingsministeriet

GRUND- OG NÆRHEDSNOTAT TIL FOLKETINGETS EUROPAUDVALG

Kommissions meddelelse "Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed ("EU's akademi for cybersikkerhedskompetencer")" (KOM (2023) 207)

Nyt notat

1. Resumé.

Meddelelsen blev fremsat den 18. april 2023 og oversendt i dansk sprogversion den 23. maj. Den beskriver trusselsbilledet og den akutte mangel på cybersikkerhedskompetencer i EU's medlemslande. Dette udfordrer EU's modstandsdygtighed, konkurrenceevne og vækst, som bl.a. afhænger af en kvalificeret arbejdsstyrke indenfor cybersikkerhed. Meddelelsen beskriver årsager til manglen og den fragmenterede tilgang til emnet i EU. På den baggrund skitserer Kommissionen, hvordan man agter at afhjælpe manglen på cybersikkerhedskompetencer igennem oprettelsen af et akademi for cybersikkerhedskompetencer.

Akademiet for cybersikkerhedskompetencer har som mål at skabe synergi mellem nationale og europæiske initiativer og fungere som et fælles kontaktpunkt for udbud af uddannelser indenfor cybersikkerhed samt finansieringsmuligheder og foranstaltninger til støtte for udviklingen af cybersikkerhedskompetencer. Akademiet skal udbygge interessenternes initiativer for dermed at nå en kritisk masse, der kan have en effekt på arbejdsmarkedet, herunder vedrørende cyberforsvar. Endelig skal aktiviteterne afstemmes efter fælles mål og centrale resultatindikatorer med henblik på at opnå større virkning. Akademiet for cybersikkerhedskompetencer er bygget op omkring fire søjler 1) Fremme af vidensopbygning gennem uddannelse, 2) Sikring af en bedre formidling og synlighed vedrørende tilgængelige finansieringsmuligheder, 3) Opfordring til interessenterne om at igangsætte tiltag, 4) fastlæggelse af indikatorer til overvågning af udviklingen på markedet.

Regeringen hilser meddelelsen velkommen, herunder fokusset på at sikre kønsmæssig konvergens i jobs inden for cybersikkerhed. Regeringen anerkender den akutte mangel på cybersikkerhedskompetencer i EU's medlemslande og vigtigheden heraf for EU og Danmarks sikkerhed og konkurrenceevne. Regeringen finder det vigtigt, at initiativer på området sker med respekt for national kompetence på uddannelsesområdet samt de videregående uddannelsesinstitutioners autonomi. Regeringen kan acceptere den foreslåede finansiering igennem programmet for et Digitalt Europa, men ser behov for yderligere uddybelse af finansieringsmodellen for akademiet igennem en EDIC. Regeringen mener, at lokal forankring er essentielt for at opnå meddelelsens formål. Såfremt der lægges op til at forankre akademiet i medlemslandene, mener regeringen at dette bør tænkes ind i de eksisterende institutionelle rammer. Regeringen finder det vigtigt, at medlemslandene inddrages behørigt i udarbejdelsen af nye indikatorer under DESI og nye centrale resultatindikatorer under politik programmet for det digitale årti 2030, og mener at dette bør gøres i medlemsstatsudvalget herfor, fremfor i en meddelelse fra Kommissionen.

2. Baggrund

Europa-Kommissionen (Kommissionen) har den 18. april 2023 præsenteret meddelelsen "Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed ("EU's akademi for cybersikkerhedskompetencer")" (KOM (2023) 207). Meddelelsen blev modtaget i dansk sprogversion den 23. maj 2023.

Meddelelsen blev fremsat som en del af Kommissionens Cybersikkerhedspakke, der også indeholder forslaget til en forordning om foranstaltninger til styrkelse af solidariteten og kapaciteten i Unionen til at opdage, forberede sig og reagere på cybersikkerhedstrusler og -hændelser, KOM (2023) 209, samt en ændring af Cybersikkerhedsforordningen, KOM (2023) 208. Europa-Kommissionens formand Ursula von der Leyen udtrykte sin hensigt om at oprette et sådan akademi i sin tale om Unionens tilstand i 2022.

Akademiet supplerer de to rådshenstillinger vedrørende digital uddannelse og digitale færdigheder1, som Kommissionen offentliggjorde samtidig med meddelelsen. Meddelelsen skal desuden ses i sammenhæng med politikprogrammet for det digital årti 2030[2], hvor der er fastsat et fælles mål om at øge antallet af IKT-fagfolk i EU med ca. 150 mio. DKK frem til 2030, samtidig med at der sikres konvergens imellem kønnene.

Bagtæppet for meddelelsen er, at trusselsbilledet vedrørende cybersikkerhed har udviklet sig betydeligt i de seneste år, og der ses et stigende antal cyberangreb rettet mod kritisk militær og civil infrastruktur i EU. Trusselsaktørerne bliver stadig dygtigere, og nye hybride trusler dukker op såsom brugen af bots og teknikker baseret på kunstig intelligens. Dertil har de geopolitiske spændinger i forbindelse med Ruslands angrebskrig mod Ukraine øget cybersikkerhedstruslen. Kommissionen mener derfor, at EU har et akut behov for fagfolk med de færdigheder og kompetencer, der er nødvendige for at forebygge, afsløre, afværge og forsvare EU mod cyberangreb, herunder kritisk infrastruktur, og dermed sikre EU's modstandsdygtighed. De manglende kompetencer inden for cybersikkerhed hæmmer desuden Europas konkurrenceevne og vækst, som i stigende grad hænger sammen med digitalisering.

For at afhjælpe manglen på cybersikkerhedskompetencer på arbejdsmarkedet foreslår Kommissionen at oprette Akademiet for cybersikkerhedskompetencer. Opstarten af akademiet støttes med 75 mio. DKK fra programmet for et Digital Europa. Midlerne er allerede afsat i det færdigforhandlede arbejdsprogram for 2023/2024.

Akademiet for cybersikkerhedskompetencer kan på sigt tage form af et europæiske konsortium for digital infrastruktur (EDIC), således at projektets levetid kan strække sig ud over EU's flerårige finansielle ramme og kontinuiteten dermed sikres.

Den 30. maj var der frist for, at interesserede medlemsstater kunne indsende en frivillig præ-notifikation om deres potentielle fremtidige ansøgning til den pågældende EDIC. Digitaliserings – og Ligestillingsministeriet (DLM) har tilkendegivet interesse for oprettelse af en EDIC for cyberkompetencer. Der er endnu ikke fastsat en dato for hvornår der skaltræffes en endelig beslutning om deltagelse i den pågældende EDIC. Dog arbejder man på at færdiggøre EDIC for cyberkompetencer i efteråret 2023.

Mens EDIC formelt oprettes, etablerer Kommissionen et virtuelt fælles kontaktpunkt ved at styrke Kommissionens platform for digitale færdigheder og job med støtte fra projektet European Cybersecurity Community Support (ECCO).

Det Europæiske Agentur for Cybersikkerhed (ENISA) bidrager til realiseringen af akademiet i overensstemmelse med agenturets målsætninger, navnlig med hensyn til bistand inden for uddannelse i cybersikkerhed. Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC) støtter i overensstemmelse med sin strategiske dagsorden realiseringen af akademiet for cybersikkerhedskompetencer.

3. Formål og indhold

Akademiet har til formål at øge færdighederne inden for cybersikkerhed for fagfolk i EU. Målet er at reducere manglen på cybersikkerhedskompetencer og sikre EU den nødvendige arbejdsstyrke, for at beskytte EU mod cyberangreb, og styrke forretningsmulighederne og konkurrenceevnen. Kommissionen mener, at en kvalificeret arbejdsstyrke inden for cybersikkerhed særligt vil være til gavn for civilsamfund, forsvar, diplomati og retshåndhævelse og fremme synergier herimellem.

Akademiet for cybersikkerhedskompetencer er bygget op omkring fire søjler:

1. Fremme af vidensopbygning gennem uddannelse

[1] Forslag til rådshenstilling om de vigtigste støttefaktorer for vellykket digital uddannelse KOM (2023) 205 og Forslag til rådshenstilling om forbedring af udbuddet af digitale færdigheder inden for uddannelse KOM (2023)206.
[2] EUROPA-PARLAMENTETS OG RÅDETS AFGØRELSE (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030

2. Sikring af en bedre formidling og synlighed vedrørende tilgængelige finansieringsmuligheder
3. Opfordring til interessenterne om at igangsætte tiltag
4. Fastlæggelse af indikatorer til overvågning af udviklingen på markedet

Første søjle: Fremme af vidensopbygning gennem uddannelse

Under akademiet for cybersikkerhedskompetencer vil der blive udviklet en struktureret tilgang til atøge antallet af personer med cybersikkerhedskompetencer i EU. Under akademiet vil man desuden målrette uddannelser mod markedsbehovene og skabe synlighed om karriereforløb.

Kommissionen ønsker at etablere en fælles tilgang til rolleprofiler inden for cybersikkerhed og de dertil knyttede færdigheder. ENISA har indledt arbejdet med at definere rolleprofiler for fagpersoner inden for cybersikkerhed som en del af European Cyber Skills Competence Framework (ECSF). Profilerne skal benyttes som grundlag for at definere og vurdere relevante færdigheder. De skal desuden bruges til at overvåge udviklingen vedrørende kompetencemanglen og afdække nye behov. ECSF vil regelmæssigt blive suppleret og revideret under akademiet i en toårig cyklus. Det er ligeledes hensigten at sikre sammenhæng mellem ECSF og relevante instrumenter under EU's beskæftigelsespolitik, herunder vil jobprofilerne under ECSF og de tilhørende færdigheder blive integreret i det europæiske klassifikationssystem for kompetencer/færdigheder, kvalifikationer og stillingsbetegnelser (ESCO-klassifikationen). Kommissionen beskriver, at klassificeringen af roller og færdigheder inden for cybersikkerhed vil gøre det lettere for enkeltpersoner at opkvalificere og omskole sig, samt at lave færdighedsbaseret jobmatchning på tværs af grænser.

Kommissionen ønsker at akademiet på sigt skal drives med finansiel støtte fra medlemsstaterne igennem en EDIC, som hver enkelt medlemsland selv beslutter, om man vil indgå i. Dette med henblik på at blive referencepunktet i Europa for udformning og levering af cybersikkerhedskurser, og på at tilbyde uddannelses- og oplæringsmuligheder. EDICen om cyberkompetencer bør ifølge Kommissionen samarbejde med alle relevante interessenter, herunder erhvervslivet, om at udforme uddannelserne og videreføre projekter der allerede finansieres af programmet for et Digitalt Europa. Akademiet for cybersikkerhedskompetencer vil særligt samarbejde med interessenter om at tiltrække unge. Til dette formål opfordrer Kommissionen medlemsstaterne til at indføre og styrke foranstaltninger til at rekruttere og uddanne specialiserede undervisere og gøre det lettere at opnå færdigheder inden for cybersikkerhed, herunder gennem lærings- og praktikforløb. Kommissionen vil fortsat yde støtte til udvikling af mikroeksamensbeviser og erhvervsuddannelsesprogrammer.

Kommissionen opfordrer de nationale cyberkoordinationscentre (NCC'erne) til at undersøge muligheden for at oprette cyberinstitutter i medlemsstaterne, da det ifølge Kommissionen vil lette samarbejdet på nationalt plan mellem den akademiske verden og udbydere af uddannelse i cybersikkerhedsfærdigheder. Ifølge Kommissionen skal cyberinstitutterne have som mål at fungere som ekspertisecentre på nationalt plan for cybersikkerhedsområdet.

Ifølge Kommissionen vil ENISA også forbedre sit tilbud om uddannelse i cybersikkerhed ved at tilpasse sit kursuskatalog til ECSF-profilerne og udarbejde uddannelsesmoduler for hver profil. Endvidere vil ENISA udvide sit "train the trainer"-program, der er målrettet de faglige behov hos EU's institutioner, medlemsstaternes offentlige myndigheder og kritiske operatører inden for den offentlige og private sektor. Derudover vil Det Europæiske Sikkerheds- og Forsvarsakademi (ESDC) udvikle og tilpasse cybersikkerhedskurser til ECSF. ESDC vil i samarbejde med Kommissionen undersøge muligheden for at integrere cybersikkerhedscertifikater i EU's eID-tegnebog.

Akademiet for cybersikkerhedskompetencer skal sikre synlighed og synergi i forbindelse med uddannelse og certificering. Kommissionen mener, at det vil fremme cyberkompetencer inden for både civilsamfundet og forsvar, retshåndhævelse og diplomati, da de forskellige sektorer ofte har brug for den samme ekspertise baseret på de samme læseplaner og læringsresultater.

Det er Kommissionens ambition at akademiet vil fungere som et fælles kontaktpunkt for dem, der er interesseret i en karriere inden for cybersikkerhed. På kort sigt kan det gøres ved at styrke Kommissionens platform for digitale færdigheder og job med støtte fra ECCO-projektet. En særlig sektion om karrierer inden for cybersikkerhed kan skabe sammenhæng med eksisterende værktøjer. Sektionen skal både dække over jobmuligheder, videregående uddannelsesprogrammer, erhvervsuddannelsesprogrammer og andre uddannelsestilbud, herunder kurser med tilhørende mikroeksamensbevis.

Ifølge Kommissionen vil ENISA udvikle et pilotprojekt for at afprøve etableringen af en europæisk attesteringsordning for cybersikkerhedsfærdigheder, så fagfolk har en sikkerhed for, at de kurser, de gennemfører, er af den krævede kvalitet.

Anden søjle: Sikring af en bedre formidling og synlighed vedrørende tilgængelige finansieringsmuligheder

Under akademiet for cybersikkerhedskompetencer vil effekten af investeringer i cybersikkerhedsfærdigheder blive maksimeret ved at skabe et samlet overblik over finansieringsmuligheder. Akademiet vil derudover fremme en bedre fordeling af midlerne efter markedets behov og strømline anvendelsen af finansiering.

ECCC vil med støtte fra Kommissionen, ECCO-projektet og de nationale cyberkoordinationscentre indsamle information om, hvordan EU-midlerne anvendes til finansiering af cybersikkerhedskompetencer. Herefter vurderes det, hvordan EU-midlerne bedst afhjælper manglen på samme. Derudover ønsker Kommissionen at synliggøre tilgængelige midler og initiativer indenfor cybersikkerhedskompetencer på platformen for digitale færdigheder og job.

Medlemsstaterne opfordres af Kommissionen til at mobilisere deres direkte forvaltede EU-midler til støtte for cybersikkerhedsfærdigheder og jobs inden for området.

Tredje søjle: Opfordring til interessenterne om at igangsætte tiltag

Kommissionen opfordrer interessenter til at give konkrete tilsagn om at opkvalificere og omskole arbejdstagere gennem målrettede foranstaltninger, der så vidt muligt afhjælper manglen på cybersikkerhedskompetencer. Sådanne tilsagn bør indberettes via platformen for digitale færdigheder og job.

Kommissionen opfordrer endvidere medlemsstaterne til at videreføre indsatsen for at gennemføre erklæringen Women in Digital samt til at udvikle synergier med programmerne under Den Europæiske Socialfond+ (ESF+) f.eks. ved at etablere mentorprogrammer for piger og kvinder.

Ifølge Kommissionen bør medlemsstaterne som led i de nationale cybersikkerhedsstrategier vedtage specifikke foranstaltninger til at afhjælpe manglen på cybersikkerhedskvalifikationer. De bør desuden identificere og forbedre formidlingsindsatsen for at afhjælpe kvalifikationsmanglen og derigennem sikre korrekt gennemførelse af forpligtelserne i henhold til NIS2-direktivet. Kommissionen tilskynder desuden medlemslandene til at drøfte initiativer og opfordrer dem til at vurdere, hvordan en kvalificeret arbejdsstyrke bedst kan tjene både forsvaret og civilsamfundet, når det gælder cybersikkerhed.

Fjerde søjle: Fastlæggelse af indikatorer til overvågning af udviklingen på markedet

Akademiet vil udvikle en metode til at måle fremskridtene med at afhjælpe manglen på cybersikkerhedskompetencer. ENISA vil i samarbejde med Kommissionen og NIS-samarbejdsgruppen udvikle indikatorer til at følge udviklingen. Indikatorerne vil blive integreret i Kommissionens indeks over den digitale økonomi og samfund (DESI).

Ifølge Kommissionen vil ENISA indsamle data om indikatorerne med støtte fra ECCO-projektet og de nationale cyberkoordinationscentre. Baseret på de indsamlede data vil ENISA udarbejde en årlig rapport, som kan indgå i statusrapporten om det digitale årti, som sammen med DESI indgår i de landespecifikke anbefalinger, der udarbejdes under det europæiske semester. ENISA vil desuden i tæt samarbejde med Kommissionen og de nationale cyberkoordinationscentre foreslå centrale resultatindikatorer (KPIer) til Kommissionen på grundlag af metodologien fra politik programmet for det digitale årti 2030.

4. Europa-Parlamentets udtalelser

Europa-Parlamentet har ikke forholdt sig til meddelelsen.

5. Nærhedsprincippet

Der redegøres ikke for nærhedsprincippet, idet der alene er tale om en meddelelse fra Kommissionen.

6. Gældende dansk ret

Ikke relevant.

7. Konsekvenser

Lovgivningsmæssige konsekvenser

Kommissionens meddelelse har ikke i sig selv konsekvenser for dansk ret.

Økonomiske konsekvenser

Meddelelsen har ikke i sig selv erhvervsøkonomiske, samfundsøkonomiske eller statsfinansielle konsekvenser. Akademiet finansieres med ca. 75 mio. DKK fra programmet for et Digital Europa. Disse midler er allerede afsat i det færdigforhandlede arbejdsprogram for 2023/2024.

Det kan forventes, at oprettelsen af EU's akademi for cybersikkerhedskompetencer kan have en positiv økonomisk effekt på dansk erhvervsliv ved at imødekomme manglen på cybersikkerhedskompetencer.

Såfremt det fra dansk side besluttes at støtte en EDIC for cyberkompetencer vil det have statsfinansielle konsekvenser, da en sådan indebærer udgifter for den danske stat. Det er ikke muligt at kvantificere disse nærmere på nuværende tidspunkt. Det bemærkes, at afledte nationale udgifter som følge af EU-retsakter afholdes inden for de berørte ministeriers eksisterende bevillingsramme, jf. budgetvejledningens bestemmelser herom.

Andre konsekvenser og beskyttelsesniveauet

Meddelelsen har ikke i sig selv konsekvenser for beskyttelsesniveauet. Et højere niveau af cybersikkerhedskompetencer i befolkningen vurderes dog at kunne få positiv effekt på modstandsdygtigheden.

8. Høring

Meddelelsen har været sendt i høring i EU-specialudvalget for konkurrenceevne, vækst og forbrugerspørgsmål, EU-specialudvalget for civilbeskyttelse og EU-specialudvalget for ungdom og uddannelse med frist for bemærkninger den 19. juni 2023. Der er kommet høringssvar fra Dansk Industri, F&P, Finanssektorens Arbejdsgiverforening, Aalborg Universitet, Dansk Erhverv og Region Midtjylland.

Høringssvarene fra henholdsvis Dansk Industri, F&P, Finanssektorens Arbejdsgiverforening, Aalborg Universitet og Dansk Erhverv forholder sig positivt til meddelelsen, og giver udtryk for en anerkendelse af manglen på cybersikkerhedskompetencer i EU.

Dansk Industri

Dansk Industri påpeger desuden, at der dog er grund til at være opmærksom på, hvordan procedurerne kan tilrettelægges mere simpelt og med inddragelse af færre instanser.

F&P

F&P finder det særligt positivt, at Europa-Kommissionen i meddelelsen ikke kun har fokus på uddannelse af kommende arbejdskraft, men også indtænker opkvalificering af den nuværende arbejdsstyrke i initiativet. F&P finder at der er behov for at indtænke efteruddannelse af den nuværende arbejdsstyrke i løsningen, hvis udfordringen med manglen på cybersikkerhedskompetencer skal imødekommes. Særligt i lyset af de krav, som virksomhederne skal leve op til i forbindelse med implementeringen af NIS2 og DORA.

Dertil finder F&P det positivt, at der med initiativet etableres en infrastruktur, der kan fungere som et fælles kontaktpunkt til fremme af samarbejdet mellem den akademiske verden, uddannelsesudbydere og industrien, hvor udbuds- og efterspørgselssiden af EU's cybersikkerhedsøkosystem kan mødes og uddannes. Styrket offentlig-privat samarbejde er en nøgle til at løse problemstillingen.

I forlængelse heraf er F&P positive over for Europa-Kommissionens forslag om at etablere nationale cyberinstitutter, som kan fungere som ekspertisecentre på nationalt plan på cybersikkerhedsområdet, og understøtte samarbejdet mellem den akademiske verden og udbydere af uddannelse i cybersikkerhedskompetencer og arbejdsgivere i den private og offentlige sektor.

F&P finder det bekymrende, at der lægges op til, at den nationale implementering af initiativet skal forankres i de nationale cyberkoordinationscentre, der etableres som led i implementeringen af NIS2-direktivet. Manglen på cybersikkerhedskompetencer er et samfundsproblem, der går udover NIS2 direktivets genstandsfelt og de selskaber, som er underlagt direktivet. Eksempelvis er der også et stort behov for cybersikkerhedskompetencer i den finansielle sektor, der ikke er omfattet af NIS2-direktivet men DORA. F&P finde det derfor vigtigt, at initiativet tænkes bredere end NIS2-initiativet.

Dansk Erhverv

Dansk Erhverv er enige i betragtningen om, at EU's sikkerhed og konkurrenceevne afhænger af, at der er adgang til en kvalificeret arbejdsstyrke indenfor cybersikkerhed. Derfor støtter Dansk Erhverv også formålet om at skabe synergi og koordination på EU-niveau, så initiativer kan opnå en kritisk masse og gøre en reel forskel. Dog pointerer Dansk Erhverv, at arbejdet på europæisk niveau ikke må tage ressourcer fra eller på anden måde reducere nationale tiltag i Danmark, da vi i høj grad har brug for at øge kapaciteten.

Region Midtjylland

Region Midtjylland kritiserer at tilgangen i meddelelsen i høj grad er, at jobs inden for cybersikkerhed er en meget afgrænset og selvstændig disciplin for folk, som ikke arbejder med andet. Region Midtjylland pointerer, at der kan vindes meget på at tænke bredere og gøre cyber- og informationssikkerhed til en del af andre (it-)uddannelser.

Region Midtjylland pointerer, at efterlevelsen af NIS2 kræver medarbejdere med forståelse for cybersikkerhed, men at der f.eks. også er krav om at ledelsen følger kurser, så de opnår tilstrækkelige kundskaber og færdigheder. Region Midtjylland forestiller sig, at EU fremadrettet vil stille mere detaljerede krav til kurser/certificeringer/uddannelse for flere typer af medarbejdere, hvis de lykkes med at standardisere jobprofiler og tilhørende kompetencer

Region Midtjylland mener at "de uberettiget oversete tværfaglige færdigheder" der nævnes i meddelelsen, i høj grad er færdigheder, der findes blandt akademiske generalister, der ofte uddannes netop til færdigheder frem for specifikke stillinger. Det er samtidig en gruppe, der generelt – i hvert fald i Danmark – oplever vanskeligheder i overgangen fra uddannelse til et arbejdsmarked, der i vid udstrækning efterspørger erfarne kandidater med en mere specifik uddannelsesprofil. Det er også et vilkår på cybersikkerhedsområdet (og på informationssikkerhedsområdet), at der i høj grad efterspørges medarbejdere med erfaring inden for området, hvilket dels, ikke står mål med arbejdsstyrkens kompetencer, og dels, som det også nævnes, modvirker at arbejdsstyrken kan opbygge de kompetencer der efterspørges.

Region Midtjylland vurderer at det er meget positivt, at der er fokus på livslang læring, og at det fokus godt kan udvides yderligere, da der er nogle meget sunde synergieffekter ved at bygge cybersikkerhedskompetencer oven på eksisterende fagligheder med flere års erfaring fra fx sundhedsområdet.

Region Midtjylland mener, at standardiserede uddannelser til en vis grad vil gøre det nemmere for regionen at rekruttere de rette "autoriserede" kompetencer, men oplever det ikke som noget stort problem i dag. Regionen anvender heller ikke konsekvent de jobbetegnelser, som ENISA har udarbejdet. Vejledning fra ENISA om jobprofiler og indhold kan måske være en hjælp for regionen, men regionen vil være sig selv nærmest ift. at vide hvilke kompetencer der er brug for, så Region Midtjylland mener ikke at ENISAs jobprofiler må blive dikterende.

Region Midtjylland mener at standardiserede uddannelser, som sigter mod at give de studerende de kompetencer de skal have for at varetage et bestemt jobfunktion, vil gøre det nemmere for studerende, at vide hvad de kan bruge en bestemt uddannelse til. Dog mener Region Midtjylland, at behovet for nogle kompetencer ændrer sig med samme fart som teknologien, og det næsten virker utænkeligt at EU og uddannelsesinstitutionerne kan følge med i samme takt, hvis det skal ske i en "toårig cyklus". Region Midtjylland mener dog ikke at det er forskelligt fra andre certificerede uddannelser, der allerede udbydes.

9. Generelle forventninger til andre landes holdninger

Ét land har meldt sig til at stå i spidsen for at oprette en EDIC for cyberkompetencer, som skal danne rammerne for samarbejdet om EU's akademi for cybersikkerhedskompetencer. Derudover har en lille håndfuld lande også givet udtryk for at de vil tilslutte sig samarbejdet.

En større gruppe lande forholder sig skeptisk til oprettelsen af akademiet, selvom de anerkender problemstillingen om mangel på cybersikkerhedskompetencer.

10. Regeringens foreløbige generelle holdning

Regeringen hilser meddelelsen velkommen, herunder fokusset på at tilskynde kvinder til at spille en aktiv og fremtrædende rolle i sektoren for digital teknologi og sikre kønsmæssig konvergens i jobs inden for cybersikkerhed. Regeringen anerkender den akutte mangel på cybersikkerhedskompetencer i EU's medlemslande og vigtigheden

heraf for EU og Danmarks sikkerhed og konkurrenceevne. Det er dog vigtigt for regeringen, at europæiske initiativer på området skaber merværdi og reelt bidrager til at afhjælpe manglen på cybersikkerhedskompetencer.

Regeringen finder det vigtigt, at initiativer på området sker med respekt for national kompetence på uddannelsesområdet samt de videregående uddannelsesinstitutioners autonomi.

Regeringen ser behov for yderligere uddybelse af finansieringsmodellen for akademiet, herunder om en EDIC er det bedste værktøj til at drive akademiet på lang sigt. Regeringen finder det ligeledes vigtigt at adgangen til akademiet ikke afhænger af deltagelse i en evt. EDIC, da opstarten af akademiet finansieres af EU-midler via programmet for et Digital Europa. Regeringens endelige stillingtagen til deltagelse i den kommende EDIC afventer således en nærmere vurdering af de statsfinansielle, samfunds- og erhvervsøkonomiske konsekvenser.

Regeringen finder det uklart i hvilken grad og hvordan akademiet vil blive forankret lokalt i de deltagende medlemslande. Det er regeringens holdning, at lokal forankring er essentielt for at opnå de resultater, som meddelelsen, herunder EDIC for cyberkompetencer ønsker at opnå. Såfremt der lægges op til at forankre akademiet i medlemslande, bør dette tænkes ind i de eksisterende institutionelle rammer.

Regeringen finder det vigtigt, at initiativerne i meddelelsen kommer samfundet bredt set til gode, herunder at erhvervslivet inkluderes tidligt og ofte i udformningen af akademiet, så dets indsatser målrettes de kompetencer, der er konkret efterspørges i erhvervslivet.

Regeringen kan acceptere den foreslåede finansiering af forslaget igennem 2023/2024 arbejdsprogrammet for et digitalt Europa. Regeringen mener generelt, at midler under programmet for et digitalt Europa skal fordeles i en sammenhængende prioritering i den dertil nedsatte programkommité. Prioriteringer af midler inden for programmet for et digitalt Europa bør generelt foretages på en sammenhængende, inkluderende og transparent måde frem for i Kommissions meddelelser og retsakter.

Regeringen finder det vigtigt, at medlemslandene inddrages behørigt i udarbejdelsen af nye indikatorer under DESI og nye centrale resultatindikatorer under politik programmet for det digitale årti 2030, og mener at beslutninger om behovet for sådanne bør træffes i medlemsstatsudvalget herfor på baggrund af en sammenhængende prioritering, fremfor i en meddelelse fra Kommissionen.

11. Tidligere forelæggelse for Folketingets Europaudvalg

Sagen har ikke tidligere været forelagt Folketingets Europaudvalg.