EUROPA-
KOMMISSIONEN

Strasbourg, den 18.4.2023
COM(2023) 207 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed ("EU's akademi for cybersikkerhedskompetencer")

Opbygning af cybersikkerhedskompetencer skal styrke EU's konkurrenceevne, vækst og modstandsdygtighed ("EU's akademi for cybersikkerhedskompetencer")

1. Der er akut behov for at reducere risici ved at afhjælpe manglen på cybersikkerhedskompetencer

Cybersikkerhed er ikke kun vigtig for borgernes, virksomhedernes og medlemsstaternes sikkerhed. Cybersikkerhed er også afgørende for at sikre EU's politiske stabilitet, stabiliteten i demokratierne og velstanden i vores samfund og virksomheder. **Trusselsbilledet** vedrørende cybersikkerhed har udviklet sig betydeligt i de seneste år, og der ses en bekymrende tendens til, at et stigende antal cyberangreb er 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[1]. Navnlig forvolder trusselsaktørerne betydelig skade for forskellige enheder, både hvad angår økonomi og omdømme, ved rutinemæssig anvendelse af ransomware[2].

Et stort antal cybersikkerhedshændelser har også været rettet mod offentlige forvaltninger og regeringer i medlemsstaterne samt EU's institutioner, organer, kontorer og agenturer[3]. Finanssektoren[4] og sundhedssektoren[5], der begge er essentielle for samfundet og økonomien, har også konsekvent været udsat for angreb[6]. De geopolitiske spændinger i forbindelse med Ruslands angrebskrig mod Ukraine har øget cybersikkerhedstruslen[7] og kan destabilisere vores samfund. EU's **sikkerhed** kan ikke garanteres uden **EU's mest værdifulde aktiv** — **befolkningerne.** EU har akut behov for fagfolk med de færdigheder og kompetencer, der er nødvendige for at forebygge, afsløre og afværge og forsvare EU mod cyberangreb, herunder kritisk infrastruktur, og sikre EU's **modstandsdygtighed**.

De manglende kompetencer inden for cybersikkerhed hæmmer desuden Europas **konkurrenceevne** og **vækst**, som i høj grad afhænger af udviklingen og udbredelsen af strategiske digitale teknologier (f.eks. kunstig intelligens, 5G og cloudløsninger). Der er behov for en kvalificeret arbejdsstyrke inden for cybersikkerhed, for at EU fortsat kan være i stand til at levere centrale avancerede teknologier i en global sammenhæng.

---

[1] ENISA's trusselsrapport: ENISA Threat Landscape 2022 — ENISA (europa.eu)

[2] Undersøgelse fra Europol: Internet Organised Crime Threat Assessment (IOCTA) 2021. Disse aktører benytter modellen Ransomware-as-a-service. De årlige omkostninger for virksomhederne oversteg i 2022 18,4 mia. EUR (Cybereason 2022 Report on the true cost or Ransomware).

[3] Se f.eks. Fælles publikation fra ENISA og CERT-EU, JP-23-01 - Sustained Activity by Threat Actors, TLP:CLEAR, 15. februar 2023.

[4] I Tyskland var 90 % af de tilfælde af e-mailsvindel, der blev indberettet fra den 1. juni 2021 til den 31. maj 2022, phishing af finansielle oplysninger, og et angreb på en virksomhed i den finansielle sektor omfattede over 20 000 inficerede enheder i 125 lande. Se rapporten The State of IT Security in Germany in 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. januar 2023

[5] I Frankrig ses eksempler på ransomwareangreb på offentlige sundhedsenheder såsom Centre Hospitalier Sud Francilien, hvor 11 GB personoplysninger, sundhedsoplysninger og personaleoplysninger blev lækket og offentliggjort af trusselsaktøren. Se rapporten Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), januar 2023

[6] ENISA's Trusselsbillede 2022

[7] Se også: CERT-EU – Russia's war on Ukraine: one year of cyber operations (europa.eu); Russiske cyberoperationer over for Ukraine:erklæring fra den højtstående repræsentant på Den Europæiske Unions vegne, 10. maj 2022 Erklæring fra den højtstående repræsentant på Den Europæiske Unions vegne om ondsindede cyberaktiviteter, der udføres af hackere og hackergrupper i forbindelse med Ruslands aggressionskrig mod Ukraine, 19. juli 2022.

For at forberede sig og imødegå et trusselsbillede i konstant udvikling og for at styrke EU's konkurrenceevne har der i de seneste år været fokus på EU's cybersikkerhedspolitik, og det har ført til vedtagelsen af en række initiativer såsom EU's strategi for cybersikkerhed for det digitale årti[8], det reviderede direktiv om net- og informationssikkerhed (NIS2-direktivet)[9], EU's sektorspecifikke lovgivning om cybersikkerhed[10], EU's politik for cyberforsvar[11], forordningen om cyberrobusthed[12] og forordningen om cybersolidaritet, som Kommissionen fremsætter forslag til sammen med denne meddelelse. Men uden de nødvendige kvalificerede personer til at gennemføre retsakterne vil målsætningerne ikke kunne opfyldes. Befolkningens grundlæggende viden om cybersikkerhed hører under initiativer vedrørende opbygning af generelle færdigheder, der er nødvendige for at deltage i samfundet[13], men samtidig er det afgørende at have en kompetent arbejdsstyrke i både den offentlige og den private sektor på nationalt plan og EU-plan, herunder i standardiseringsorganisationer, for at **kunne opfylde de lovgivningsmæssige og politiske krav vedrørende cybersikkerhed**.

EU's sikkerhed og konkurrenceevne afhænger derfor af, at der er en kvalificeret arbejdsstyrke inden for cybersikkerhed. Der er imidlertid i EU en meget betydelig mangel på kvalificerede fagfolk inden for cybersikkerhed, hvilket indebærer risiko for cybersikkerhedshændelser for EU, medlemsstaterne, virksomhederne og borgerne i EU. I 2022 blev manglen på kvalificerede fagfolk inden for cybersikkerhed i EU anslået til **mellem 260 000**[14] **og 500 000**[15], samtidig med at EU's behov for en kvalificeret arbejdsstyrke inden for cybersikkerhed blev anslået til 883 000 kvalificerede fagfolk[16], og der er dermed et misforhold mellem de kompetencer, der er til rådighed, og dem, der er behov for på arbejdsmarkedet. Der er desuden den fejlagtige opfattelse af cybersikkerhedsområdet, at det er stærkt teknisk, og derfor søger kun få kvinder inden for området. Kvinder tegner sig således kun for 20 % af de færdiguddannede inden for cybersikkerhed[17] og 19 % af specialisterne inden for informations- og kommunikationsteknologi (IKT)[18]. For at afhjælpe

---

[8] Fælles meddelelse til Europa-Parlamentet og Rådet — EU's strategi for cybersikkerhed for det digitale årti, JOIN(2020) 18 final.

[9] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet)

[10] Som f.eks. vedrørende finanssektoren Europa-Parlamentets og Rådets forordning (EU) 2022/2554 af 14. december 2022 om digital operationel modstandsdygtighed i den finansielle sektor og om ændring af forordning (EF) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 og (EU) 2016/1011 (DORA-forordningen)

[11] Fælles meddelelse til Europa-Parlamentet og Rådet, EU's politik for cyberforsvar, JOIN(2022) 49 final

[12] Forslag til Europa-Parlamentets og Rådets forordning om horisontale cybersikkerhedskrav til produkter med digitale elementer og om ændring af forordning (EU) 2019/1020, COM(2022) 454 final

[13] Nogle af de relevante initiativer vedrørende befolkningens generelle digitale færdigheder: 80 % af befolkningen skal opnå grundlæggende digitale færdigheder inden 2030 som et mål i handlingsplanen for den europæiske søjle for sociale rettigheder og det digitale kompas, handlingsplanen for digital uddannelse 2021-2027, redskabet for den digitale kompetenceramme eller forslaget til Rådets henstilling om forbedring af udbuddet af digitale færdigheder inden for uddannelse.

[14] (ISC²) i Assessing Cyber Skills on the basis of the ECSF, ENISA-webinar, 16. februar 2023

[15] I henhold til European Cyber Security Organisation (ECSO) som anført i Fælles meddelelse til Europa-Parlamentet og Rådet, EU's politik for cyberforsvar, JOIN(2022) 49 final

[16] (ISC²) i Assessing Cyber Skills on the basis of the ECSF, ENISA-webinar, 16. februar 2023

[17] Databasen for videregående uddannelse inden for cybersikkerhed (CyberHEAD)

[18] Kun 19 % af IKT-specialisterne i EU er kvinder Indeks over den digitale økonomi og det digitale samfund (DESI) 2022 | Europas digitale fremtid i støbeskeen (europa.eu). Der er ingen oplysninger om andelen af kvinder i EU's arbejdsstyrke, der arbejder inden for cybersikkerhed.

dette er der i EU's **politiske program for det digitale årti 2030**[19] fastsat et mål om at øge antallet af IKT-fagfolk med 20 mio. frem til 2030, samtidig med at der sikres konvergens mellem kønnene. Desuden kræver gennemførelsen af nye EU-politikker en tilstrækkeligt kvalificeret og tilstrækkeligt stor arbejdsstyrke. For eksempel fremhævede over 42 % af IT-lederne i sektoren for finansielle tjenesteydelser manglen på kompetencer og ekspertise inden for cybersikkerhed som en central udfordring for deres virksomhed, når det drejer sig om beskyttelse mod og håndtering af cybersikkerhedshændelser[20], på et tidspunkt hvor de skal gennemføre sektorspecifik lovgivning om cybersikkerhed såsom forordningen om digital operationel modstandsdygtighed (DORA).

Arbejdsgiverne tøver med at investere i menneskelig kapital og søger i stedet efter allerede uddannede og erfarne medarbejdere, hvilket bidrager yderligere til at begrænse arbejdskraftudbuddet[21]. Arbejdskraftmanglen berører alle typer virksomheder, herunder små og mellemstore virksomheder (**SMV'er**), som udgør 99 % af alle virksomheder i EU[22]. Også de **offentlige forvaltninger** oplever store udfordringer, og de er i stort omfang udsat for og påvirkes mest af cybersikkerhedshændelser[23].

Det haster derfor med at få afhjulpet EU's kompetencemangel inden for cybersikkerhed, da EU's sikkerhed og konkurrenceevne står på spil.

2. Manglen på synergi og en koordineret indsats for at afhjælpe kompetencemanglen inden for cybersikkerhed

Der er igangsat en lang række initiativer på europæisk og nationalt plan, der gennemføres af offentlige og private enheder for at afhjælpe manglen på arbejdskraft på cybersikkerhedsområdet. Det er imidlertid en fragmenteret indsats, der ikke når op på en kritisk masse, så initiativerne kan gøre en reel forskel.

For det første er der i øjeblikket en begrænset fælles viden om sammensætningen af EU's arbejdsstyrke inden for cybersikkerhed og de tilhørende kompetencer, selvom enslydende jobprofiler inden for cybersikkerhedsområdet bør omfatte det samme sæt af kompetencer. De relevante aktørers manglende anvendelse af en fælles **europæisk referenceramme for fagfolk inden for cybersikkerhed** betyder, at der mangler et værktøj til kommunikation mellem arbejdsgivere, undervisere og politiske beslutningstagere, og at det ikke er muligt at foretage målinger og vurdere manglen på arbejdskraft inden for cybersikkerhed. Det forhindrer endvidere udformning af læseplaner for uddannelse og udarbejdelse af karriereforløb, der opfylder de politiske behov og arbejdsmarkedskravene for dem, der ønsker at arbejde inden for erhvervet. **Opkvalificering og omskoling** af arbejdsstyrken afhænger i høj grad af uddannelse og certificering inden for cybersikkerhed, der normalt udbydes af private udbydere. Det er dog vanskeligt for arbejdsstyrken at få et overblik over kvaliteten i de udbudte uddannelser i cybersikkerhed og den tilhørende certificering.

Det er nødvendigt at fastlægge uddannelses- og karriereforløb for at styrke arbejdsmarkedets udbudsside, men samtidig er **efterspørgselssiden** i øjeblikket undervurderet med hensyn til

[19] Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030, der indeholder bestemmelser om etablering af en overvågnings- og samarbejdsmekanisme, der har til formål at opfylde de fælles mål og målsætninger for Europas digitale transformation i henhold til det digitale kompas for 2030, herunder på området for kompetencer.

[20] S-RM Cyber Security Insights Report 2022.

[21] Cybersecurity Skills Development in the EU, ENISA, december 2019

[22] Definition på en SMV (europa.eu)

[23] ENISA Threat Landscape 2022 — ENISA (ENISAs trusselsrapport, europa.eu)

uddannelse af arbejdsstyrken og tilpasning til udviklingen. Branchen og de offentlige arbejdsgivere mangler fælles fora og muligheder for at samle idéer til, hvordan arbejdsstyrken bedst kan uddannes, og hvordan man **bedre kan foretage en kompetencevurdering**, navnlig i forbindelse med rekruttering. De mest efterspurgte **faglige færdigheder** vedrører cybersikkerhed helt konkret[24], herunder softwareudvikling eller cloud computing[25], men samtidig bliver de tværfaglige færdigheder helt uberettiget overset. Kritisk tænkning og analyse, problemløsning og selvforvaltning er kompetencer, der i højere grad efterspørges af arbejdsgiverne[26], og som i tiltagende grad vil blive vigtige frem til 2025[27].

Der findes allerede mange offentlige og private initiativer til investering i cybersikkerhedskompetencer, og EU **finansierer** i vid udstrækning projekter under forskellige instrumenter[28]. Den fortsatte kompetencemangel i EU rejser imidlertid spørgsmål om synlighed og virkning, og det tyder på, at kompetencerne ikke systematisk modsvarer markedets behov, og der er akut behov for en kortlægning på EU-plan. De mange finansieringskilder medfører dobbeltarbejde, og muligheder for at skalere indsatsen og opnå en reel virkning går tabt. Desuden kan aktører, der har behov for investeringer, ikke altid finde frem til de kilder, der bedst dækker deres behov.

Interessenterne har forsøgt at løse det komplekse problem med mangel på cybersikkerhedskompetencer. EU's agentur for Cybersikkerhed (ENISA) har udviklet instrumenter vedrørende rolleprofiler eller videregående uddannelse[29], Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC)[30] beskæftiger sig med cybersikkerhedskompetencer i en særlig arbejdsgruppe, Det Europæiske Sikkerheds- og Forsvarsakademi (ESDC) arbejder med cybersikkerhedskompetencer i den civile og militære arbejdsstyrke inden for rammerne af den fælles sikkerheds- og forsvarspolitik[31], private organisationer arbejder på at løse problemet[32] og cybersikkerhedscertificeringsindustrien er i gang med at udvikle en køreplan og uddannelse for at afhjælpe kompetencemanglen[33]. Medlemsstaterne søger også at løse problemet gennem en række initiativer, der spænder fra regulering[34] til etablering af cybersikkerhedsakademier[35] eller cyberinstitutter[36], ekspertisecentre for cyberkriminalitet[37] eller gennem offentlig-private partnerskaber[38]. Der er dog manglende koordinering og udnyttelse af synergier mellem de forskellige interessenters

[24] LinkedIn 2023 Most In-Demand Skills: Learn the Skills Companies Need Most

[25] Infografik fra ISACA: State of Cyber Security 2022

[26] Såsom CEDEFOP's værktøj: Skills-OVATE | CEDEFOP (europa.eu).

[27] The Future of Jobs Report, October 2020, World Economic Forum

[28] Eksempler: Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project (finansieret af Erasmus+-programmet) Projekter, der støtter Cybersecurity Competence Centre (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (finansieret under Horisont 2020), Cybersecpro project (finansieret under programmet Et Digitalt Europa).

[29] Navnlig: European Cybersecurity Skills Framework (ECSF) Databasen for videregående uddannelse inden for cybersikkerhed CyberHEAD Cyber Exercise Platform (CEP) Den europæiske cybersikkerhedsudfordring Den europæiske måned for cybersikkerhed.

[30] Europa-Parlamentets og Rådets forordning (EU) 2021/887 af 20. maj 2021 om oprettelse af Det Europæiske Industri-, Teknologi- og Forskningskompetencecenter for Cybersikkerhed og Netværket af Nationale Koordineringscentre

[31] Navnlig Cyber education, training, exercise and evaluation (ETEE) platform

[32] For eksempel arbejdsgruppe 5 under European Cybersecurity Organisation (ECSO) om "Uddannelse, kendskabsopbygning, cybermiljøer og menneskelige faktorer" organisationen DIGITALEUROPE

[33] For eksempel SANS Institute, (ISC)², ISACA

[34] For eksempel i nationale strategier for uddannelse eller cybersikkerhed

[35] For eksempel C-Academy i Portugal

[36] For eksempel Campus Cyber i Frankrig

[37] For eksempel Lithuanian Cybercrime Centre of Excellence for Training, Research & Education i Litauen (L3CE)

[38] For eksempel Microsoft's Cybersecurity Skilling Initiative

arbejde, og det lykkes ikke til fulde at påvirke arbejdsmarkedet, og derfor ses en voksende mangel på arbejdskraft inden for cybersikkerhed i EU. Der er et reelt stigende behov for øget udnyttelse af synergierne på tværs af de enheder, der arbejder med cybersikkerhed, da de nødvendige kompetencer inden for opretholdelse af cybersikkerheden, bekæmpelse af **cyberkriminalitet** og opbygning af **cyberforsvarsløsninger** ofte er de samme.

Endelig har EU i dag begrænsede muligheder for at vurdere **situationen på og udviklingen af arbejdsmarkedet for cybersikkerhed** og arbejdsstyrkens kompetencer. Medlemsstaterne og EU's institutioner, organer, kontorer og agenturer er enten afhængige af data indsamlet af private enheder eller af et bredere sæt data indsamlet på EU-plan, navnlig af Eurostat[39] og Det Europæiske Center for Udvikling af Erhvervsuddannelse (Cedefop)[40] om IKT-fagfolk. Med andre ord har EU et delvist og fragmenteret overblik over behovene, og det forhindrer EU i at formulere en samlet og konsolideret vision for situationen på arbejdsmarkedet for cybersikkerhed.

3. En koordineret tilgang på EU-plan: akademiet for cybersikkerhedskompetencer

3.1.Mål

For at afhjælpe manglen på cybersikkerhedskompetencer på arbejdsmarkedet foreslår Kommissionen at oprette **Akademiet for cybersikkerhedskompetencer** som beskrevet af Europa-Kommissionens formand i hensigtserklæringen om Unionens tilstand 2022[41, 42] og i forbindelse med det europæiske år for færdigheder.

Akademiet for cybersikkerhedskompetencer (kaldet "akademiet") har som mål at skabe **synergi og fungere som et fælles kontaktpunkt** vedrørende udbud af uddannelse i cybersikkerhed samt finansieringsmuligheder og specifikke foranstaltninger til støtte for udviklingen af cybersikkerhedskompetencer. Det skal udbygge interessenternes initiativer for dermed at nå en kritisk masse, der kan have en effekt på arbejdsmarkedet, herunder vedrørende cyberforsvar. Aktiviteterne skal afstemmes efter fælles mål og centrale resultatindikatorer med henblik på at opnå større virkning.

Akademiets fokus vil være at uddanne **fagfolk inden for cybersikkerhed**. Akademiets aktiviteter skal indgå i EU's politik for cybersikkerhed og for uddannelse og livslang læring. Det supplerer de to rådshenstillinger vedrørende digital uddannelse og digitale færdigheder, som Kommissionen har foreslået samtidig med denne meddelelse[43].

Akademiet inddeles i fire søjler: 1) fremme af **videngenerering gennem uddannelse** ved at arbejde på en fælles ramme for rolleprofiler inden for cybersikkerhed og tilknyttede færdigheder, forbedre det europæiske uddannelsestilbud for at opfylde behovene, opbygge karriereforløb og skabe synlighed og overblik over cybersikkerhedskurser og -certificeringer for at forbedre arbejdsmarkedets udbudsside, 2) sikring af en bedre formidling og synlighed vedrørende tilgængelige **finansieringsmuligheder** for kompetencerelaterede aktiviteter med henblik på at maksimere deres virkning, 3) opfordring til interessenterne om at **igangsætte tiltag** og 4) fastlæggelse af indikatorer til **overvågning af udviklingen på markedet** og sikring af kapacitet til at vurdere effektiviteten af foranstaltningerne.

---

[39] ICT specialists in employment - Statistics Explained (europa.eu)

[40] Såsom Cedefops værktøj: Skills-OVATE | CEDEFOP (europa.eu).

[41] 2022 State of the European Union Letter of Intent to President Roberta Metsola and to Prime Minister Petr Fiala

[42] Fælles meddelelse til Europa-Parlamentet og Rådet, EU's politik for cyberforsvar, JOIN(2022) 49 final

[43] Forslag til Rådets henstillinger om de vigtigste forudsætninger for vellykket digital uddannelse og om forbedring af udbuddet af digitale færdigheder på uddannelsesområdet.

Realiseringen af akademiet støttes med 10 mio. EUR fra programmet for et digitalt Europa[44].

3.2.Akademiets ledelse

Akademiet kan tage form af et **europæisk konsortium for digital infrastruktur (EDIC)**[45] og stille en infrastruktur til rådighed, der fungerer 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. Gennem instrumentet kan medlemsstaterne arbejde sammen om at afhjælpe manglen på kompetencer inden for cybersikkerhed og indgå i tæt samarbejde med Kommissionen, ENISA og Det Europæiske Kompetencecenter for Cybersikkerhed (ECCC) i overensstemmelse med deres mandater og kompetencer og inddrage alle relevante interessenter, og samtidig kan europæiske, nationale og private investeringer koordineres med et fælles mål for øje. Med henblik herpå opfordres interesserede medlemsstater til senest den 30. maj 2023 at indgive en forhåndsmeddelelse til Kommissionen om deres fremtidige ansøgning vedrørende et sådant EDIC. Den frivillige forhåndsmeddelelse vil gøre det muligt for Kommissionen at fremsætte tidlige bemærkninger om et udkast til en ansøgning vedrørende et EDIC og dermed give mulighed for hurtigere videreudvikling og formel indgivelse heraf. Gennem hele processen og i det omfang, medlemsstaterne anmoder om det, vil Kommissionen, der fungerer som projektkoordinator for flere lande, bistå i udarbejdelsen af EDIC-ansøgningen. Efter Kommissionens positive vurdering af ansøgningen og godkendelse i udvalget for programmet for det digitale årti vil Kommissionen derefter udstede en afgørelse om oprettelse af et EDIC og efterfølgende bidrage til at koordinere etableringen af det pågældende EDIC[46].

I mellemtiden, og mens EDIC formelt oprettes, etablerer Kommissionen et virtuelt fælles kontaktpunkt ved at styrke Kommissionens platform **Digital Skills and Jobs Platform**[47] med støtte fra projektet European Cybersecurity Community Support (ECCO).[48]

ENISA bidrager til realiseringen af akademiet i overensstemmelse med agenturets målsætninger[49], navnlig med hensyn til bistand inden for uddannelse i cybersikkerhed og under hensyntagen til rapporteringsforpligtelserne i henhold til NIS 2-direktivet[50]. **ECCC** støtter i overensstemmelse med sin strategiske dagsorden realiseringen af akademiet for cybersikkerhedskompetencer. ECCC vil navnlig gennemføre det strategiske mål 3 (cybersikkerhed) i programmet for et digitalt Europa. ECCC støttes af Kommissionen og medlemsstaterne gennem de **nationale koordinationscentre (NCC)**. **Samarbejdsgruppen**,

---

[44] Europa-Parlamentets og Rådets forordning (EU) 2021/694 af 29. april 2021 om programmet for et digitalt Europa og om ophævelse af afgørelse (EU) 2015/2240

[45] EDIC etableres i henhold til Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030, artikel 13 ff.

[46] Ibidem, artikel 12

[47] Home | Digital Skills and Jobs Platform (europa.eu)

[48] Se European Cybersecurity Competence Centre and Network: new EU-funded project to support the Cyber Community (europa.eu). I december 2022 undertegnede Europa-Kommissionen en kontrakt på 3 mio. EUR til støtte for EU's cyberfællesskab inden for rammerne af Det Europæiske Kompetencecenter for Cybersikkerhed. Projektet skal bidrage til EU's mål om fællesskabs- og kapacitetsopbygning med hensyn til forskning, innovation, udbredelse og industrigrundlag inden for cybersikkerhed.

[49] "ENISA støtter kapacitetsopbygning og beredskab i hele Unionen ved at bistå Unionens institutioner, organer, kontorer og agenturer samt medlemsstaterne og offentlige og private interessenter for at (...) udvikle færdigheder og kompetencer inden for cybersikkerhed." Artikel 4, stk. 3, i forordningen om cybersikkerhed

[50] Artikel 18 i NIS2-direktivet

der er nedsat i henhold til NIS2-direktivet[51], bliver hørt, hvor det er relevant. Endelig vil det være nødvendigt at samarbejde med **industrien** og den **akademiske verden** for at nå akademiets mål om at afhjælpe manglen på cybersikkerhedskompetencer.

4. Vidensopbygning og uddannelse: etablering af en fælles EU-tilgang til uddannelse i cybersikkerhed

Under søjlen for vidensopbygning og uddannelse under akademiet for cybersikkerhedskompetencer vil der blive udviklet en struktureret tilgang med det klare mål at øge **antallet** af personer med cybersikkerhedskompetencer i EU, at målrette uddannelserne bedre mod **markedsbehovene** og at skabe synlighed vedrørende **karriereforløb**.

4.1. At tale samme sprog: en fælles tilgang til rolleprofiler inden for cybersikkerhed og de tilknyttede færdigheder

ENISA har allerede indledt arbejdet med at definere rolleprofiler for fagpersoner inden for cybersikkerhed som en del af European Cyber Skills Competence Framework (**ECSF**)[52]. Akademiet skal benytte profilerne som grundlag for at definere og vurdere relevante færdigheder, overvåge udviklingen vedrørende kompetencemanglen og afdække nye behov. For hver cybersikkerhedsrolle defineret under ECSF integreres et sæt gældende færdigheder under European e-Competence Framework[53] som et element i profilbeskrivelsen[54].

ENISA vil derfor gennemgå ECSF og **identificere nye kvalifikationsbehov og mangler** i arbejdsstyrken inden for cybersikkerhed, herunder ved hjælp af avancerede værktøjer (f.eks. kunstig intelligens, big data[55] og datamining). Til den opgave arbejder ENISA under ledelse af EDIC, når det er oprettet, ECCC sammen med de nationale koordinationscentre, Kommissionen, ECCO-projektet og markedsaktørerne[56]. For så vidt angår arbejdsstyrken inden for cyberforsvar vil ENISA tage behørigt hensyn til ESDC's arbejde. På området for bekæmpelse af cyberkriminalitet vil ENISA ligeledes tage hensyn til de aktiviteter, der udføres af EU's Agentur for Uddannelse inden for Retshåndhævelse (Cepol) og Europol, og foretage en analyse af de operationelle uddannelsesbehov[57] vedrørende cyberangreb.

ECSF vil regelmæssigt blive suppleret og revideret under akademiet i en toårig cyklus. Desuden vil Kommissionen og Tjenesten for EU's Optræden Udadtil bidrage til at definere

---

[51] Europa-Parlamentets og Rådets direktiv (EU) 2022/2555 af 14. december 2022 om foranstaltninger til sikring af et højt fælles cybersikkerhedsniveau i hele Unionen, om ændring af forordning (EU) nr. 910/2014 og direktiv (EU) 2018/1972 og om ophævelse af direktiv (EU) 2016/1148 (NIS 2-direktivet)

[52] European Cybersecurity Skills Framework (ECSF) — ENISA (europa.eu). ECSF støtter identifikationen og formuleringen af opgaver, kompetencer, færdigheder og viden, der hører under de forskellige roller for fagfolk inden for cybersikkerhed i Europa. ECSF samler alle roller inden for cybersikkerhed under en række profiler, som enkeltvis gennemgår en detaljeret analyse vedrørende de tilhørende ansvarsområder, færdigheder, synergier og afhængigheder.

[53] European e-Competence Framework (e-CF) | Esco (europa.eu) e-CF sikrer den løbende sammenhæng mellem IKT-kvalifikationer og andre rammer af relevans for sektoren, bl.a. DigComp

[54] Se i den sammenhæng User Manual - European Cybersecurity Skills Framework (ECSF) - september 2022.

[55] Se f.eks. Skills-OVATE, der er udviklet af Cedefop.

[56] Agenturet vil yderligere bruge resultaterne af andre EU-finansierede projekter (f.eks. REWIRE, Data Space For Skills (DS4S), CyberSecPro, Concordia) og metoder udviklet af lignende initiativer (f.eks. "Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States", OECD-rapport udgivet den 21. marts 2023) for i fremtiden at sikre et opdateret overblik over behovene i en verden, hvor efterspørgslen hele tiden ændrer sig.

[57] CEPOL Operational Training Needs Assessment (OTNA)

konkrete profiler og de tilhørende færdigheder for forskellige sektorer efter behov med støtte fra EU-agenturer og -organer såsom ESDC[58], Europol og Cepol[59].

Der sikres også sammenhæng mellem ECSF og relevante instrumenter under EU's beskæftigelsespolitik[60]. Navnlig vil jobprofilerne under ECSF og de tilhørende færdigheder blive integreret i **ESCO-klassifikationen**. Dermed forbedres klassificeringen af og sammenhængen mellem roller og færdigheder inden for cybersikkerhed, og det bliver lettere for enkeltpersoner at opkvalificere og omskole sig, og færdighedsbaseret jobmatchning og mobilitet på tværs af grænserne understøttes.

4.2. Udvikling af samarbejde om udformning af læreplaner for uddannelse i cybersikkerhed

Når det europæiske konsortium for digital infrastruktur (EDIC) er oprettet, skal akademiet modtage støtte fra medlemsstaterne med henblik på at blive **referencepunktet i Europa for udformning og levering af cybersikkerhedskurser** inden for de mest efterspurgte færdigheder, og tilbyde uddannelses- og oplæringsmuligheder på arbejdspladsen for nystartede virksomheder og SMV'er og for offentlige forvaltninger i innovative virksomheder inden for cybersikkerhed og kompetencecentre for cybersikkerhed. EDIC bør samarbejde med alle relevante interessenter, herunder industrien, om at udforme uddannelserne og videreføre projekter såsom **CyberSecPro**[61], der finansieres af programmet for et digitalt Europa, og som samler 17 videregående uddannelsesinstitutioner og 13 sikkerhedsvirksomheder fra 16 medlemsstater med henblik på at fastlægge bedste praksis for alle uddannelsesprogrammer om cybersikkerhed.

Akademiet samarbejder med alle relevante interessenter om at **tiltrække de unge generationer** til en karriere inden for cybersikkerhed. I overensstemmelse med forslaget til Rådets henstilling om forbedring af udbuddet af digitale færdigheder inden for uddannelse bør medlemsstaterne indføre og styrke foranstaltninger til at rekruttere og uddanne specialiserede lærere og undervisere og gøre det lettere at opnå færdigheder inden for cybersikkerhed, herunder gennem lærings- og praktikforløb. Integration af cybersikkerhed i uddannelsesprogrammer, samtidig med at tilgængeligheden sikres, udvikling af **læringsforløb** og praktiktilbud, fremme af innovative tilgange, herunder f.eks. seriøse spil og fælles simuleringsplatforme, tilrettelæggelse af temauger om jobroller inden for cybersikkerhed og beskrivelse af de ikke-tekniske rolleprofiler bør fremmes. Deltagelse i sådanne læringsmuligheder inden for cybersikkerhed for grupper, der er svære at nå, såsom unge med handicap, der bor i fjerntliggende områder eller landdistrikter, og andre minoritetsgrupper, bør også støttes.

Kommissionen vil fortsat yde støtte til udvikling af mikroeksamensbeviser og erhvervsuddannelsesprogrammer. Navnlig vil fælles **bachelor- og masteruddannelser,**

---

[58] Se i den forbindelse Fælles meddelelse til Europa-Parlamentet og Rådet, EU's politik for cyberforsvar, JOIN(2022) 49 final

[59] I den sammenhæng vil der blive lagt vægt på arbejdet med kompetencerammen Cybercrime Training Competency Framework (TCF), der i øjeblikket er under udvikling.

[60] For eksempel det europæiske klassifikationssystem for færdigheder, kompetencer, kvalifikationer og erhverv (ESCO), Europass og det europæiske samarbejdsnetværk for arbejdsformidlinger (EURES).

[61] CyberSecProDe vil eksempelvis gennemføre en analyse af de cybersikkerhedsprogrammer, -kurser og -sommerskoler, der tilbydes på universiteterne og i det europæiske meritoverførsels- og meritakkumuleringssystem (ECTS), sikre deltagelse af det ønskede antal på over 530 praktikanter i løbet af en periode på tre år og uddanne eksterne personer fra forskellige industrier og sektorer

fælles kurser eller moduler, der kan føre til mikroeksamensbeviser og **blandede intensive programmer**[62] om alle emner, herunder **cybersikkerhed**, fortsat blive finansieret under Erasmus+. Den videre udbredelse af **initiativet Europauniversiteter**[63] og af **erhvervsekspertisecentre**[64] vil også blive støttet for at tilskynde til øget samarbejde mellem videregående uddannelsesinstitutioner og relevante erhvervsuddannelsesinstitutioner i hele Europa. EU's finansieringsprogrammer, herunder Erasmus+ og programmet for et digitalt Europa, støtter målet om et tættere samarbejde, og det samme gælder EU-midler til udvikling af **individuelle læringskonti**[65].

For at lette samarbejdet på nationalt plan mellem den akademiske verden og udbydere af uddannelse i cybersikkerhedsfærdigheder og arbejdsgivere i den private og den offentlige sektor og fremme synergi mellem den offentlige og den private sektor opfordres de nationale koordinationscentre til at undersøge muligheden for at oprette cyberinstitutter i medlemsstaterne. Cyberinstitutterne skal have som mål at fungere som ekspertisecentre på nationalt plan for cybersikkerhedsområdet, og akademiet bidrager til deres netværkssamarbejde og den yderligere koordinering af deres aktiviteter.

ENISA vil også forbedre sit tilbud om uddannelse i cybersikkerhed ved at tilpasse **kursuskataloget**[66] til ECSF-profilerne og udarbejde uddannelsesmoduler for hver profil, hvilket kan forbedre uddannelsestilbuddene i medlemsstaterne. Endvidere vil ENISA udvide sit "**train the trainer**"-program[67], der er målrettet de faglige behov hos EU's institutioner, organer, kontorer og agenturer, medlemsstaternes offentlige myndigheder og **kritiske operatører inden for den offentlige og private sektor** inden for NIS2-direktivets anvendelsesområde.

Derudover vil andre EU-agenturer og -organer udvide deres tilbud om uddannelse i cybersikkerhed. I forbindelse med gennemførelsen af EU's politik for cyberforsvar vil **ESDC** eksempelvis udvikle en ny serie af cybersikkerhedskurser og tilpasse nogle af de nuværende kurser til ECSF. Kurserne fører til certificering af læringsresultaterne[68]. ESDC vil i samarbejde med Kommissionen undersøge muligheden for at integrere certifikater i EU's eID-tegnebog. ESDC vil yderligere undersøge mulighederne for at vurdere de færdighedsmekanismer, som certifikaterne udstedes på grundlag af. Inden for bekæmpelse af cyberkriminalitet ønskes på samme måde et tæt samarbejde med **CEPOL Cybercrime Academy**[69] for at fremme synergier og komplementaritet i udformningen og gennemførelsen af uddannelsesprogrammerne.

4.3.Synergi og synlighed vedrørende uddannelse i cybersikkerhed og certificering heraf på tværs af medlemsstaterne

[62] Blandede intensive programmer kombinerer onlineundervisning med fysisk mobilitet i en kort periode.

[63] Europauniversitet-initiativet | Det europæiske uddannelsesområde (europa.eu).

[64] Erhvervsekspertisecentre | Erasmus+ (europa.eu)

[65] I henhold til Rådets henstilling af 16. juni 2022 om individuelle læringskonti

[66] Training Courses — ENISA (europa.eu)

[67] Train the trainer programme — ENISA (europa.eu)

[68] I henhold til artikel 20, stk. 4, i Rådets afgørelse (FUSP) 2020/1515 af 19. oktober 2020 om oprettelse af Det Europæiske Sikkerheds- og Forsvarsakademi og om ophævelse af afgørelse (FUSP) 2016/2382

[69] Cepols Cybercrime Academy blev oprettet i 2019 for at tilvejebringe en avanceret platform til forbedring af viden om cyberkriminalitet og cyberkapacitet i Europa.

Akademiet skal løse opgaven med at sikre synlighed og synergi i forbindelse med uddannelse og certificering. 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.

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, lige fra videregående uddannelsesprogrammer til andre uddannelsestilbud, herunder kurser med tilhørende mikroeksamensbevis og erhvervsuddannelsesprogrammer, og jobmuligheder. Det opnås ved at henvise til eller integrere igangværende arbejde og initiativer i platformen, f.eks. initiativerne under ENISA, hvor der i samarbejde med den akademiske verden er foretaget en **kortlægning af uddannelsesinstitutioner**, der udbyder cybersikkerhedsprogrammer. Indsatsen styrkes yderligere med støtte fra de nationale koordinationscentre. Derudover udvikler og samler ENISA to **pools af eksisterende uddannelser fra den offentlige og den private sektor og af cybersikkerhedscertificeringer** med støtte fra de nationale koordinationscentre, Kommissionen og ECCO-projektet og i samarbejde med enheder, der tilbyder certificering, og baseret på andre relevante initiativer[70]. De bliver også integreret i det centrale kontaktpunkt for platformen for digitale færdigheder og job. Arbejdet vil også være til gavn for de nationale koordinationscentre, hvis opgave navnlig er at fremme og udbrede uddannelsesprogrammer om cybersikkerhed[71].

Det er også nødvendigt at give fagfolkene sikkerhed for, at de kurser, de gennemfører, er af den krævede kvalitet. I den forbindelse vil ENISA udvikle et **pilotprojekt** for at afprøve etableringen af en europæisk attesteringsordning for cybersikkerhedsfærdigheder.

Desuden er det afgørende at udpege færdigheder og uddannelser og koble dem til en jobprofil, men det er også vigtigt at sikre, at cybersikkerhedstjenesterne får adgang til den nødvendige kompetence, ekspertise og erfaring Det gælder navnlig udbydere af forvaltede sikkerhedstjenester på områder som hændelseshåndtering, penetrationstest, sikkerhedsrevisioner og konsulentbistand. I NIS2-direktivet og forslaget til forordning om cybersolidaritet er der fastsat specifikke opgaver for sådanne udbydere af forvaltede sikkerhedstjenester. Kommissionen foreslår derfor også en **målrettet ændring af forordningen om cybersikkerhed**[72] for at muliggøre certificeringsordninger for forvaltede sikkerhedstjenester på EU-plan. Sådanne certificeringsordninger bør bl.a. have som mål at sikre, at tjenesterne leveres af personale med et meget højt niveau af teknisk viden og kompetence på de relevante områder.

Kvalitetssikring og mekanismer til anerkendelse af mikroeksamensbeviser[73] øger gennemsigtigheden, sammenligneligheden og overførbarheden af læringsresultater. I

[70] For eksempel W4C Academy - Women4Cyber Academy eller Global Cybercrime Certification project for retslige og retshåndhævende myndigheder

[71] "1. De nationale koordinationscentre: (...) g) samarbejder, uden at det berører medlemsstaternes kompetencer på uddannelsesområdet og under hensyntagen til ENISA's relevante opgaver, med de nationale myndigheder om mulige bidrag til fremme og udbredelse af uddannelsesprogrammer om cybersikkerhed", artikel 7, stk. 1, litra g), i ECCC-forordningen. Se også den tilhørende betragtning 28.

[72] Europa-Parlamentets og Rådets forordning (EU) 2019/881 af 17. april 2019 om ENISA (Den Europæiske Unions Agentur for Cybersikkerhed), om cybersikkerhedscertificering af informations- og kommunikationsteknologi og om ophævelse af forordning (EU) nr. 526/2013 (forordningen om cybersikkerhed)

[73] For eksempel dokumentation for eller certifikater for læringsresultater erhvervet på kortere kurser.

overensstemmelse med Rådets henstilling om en europæisk tilgang til mikroeksamensbeviser[74] opfordres medlemsstaterne til at medtage mikroeksamensbeviser inden for cybersikkerhed i de nationale kvalifikationsrammer. Det vil gøre det muligt for dem at knytte mikroeksamensbeviser vedrørende cybersikkerhed sammen med den europæiske referenceramme for kvalifikationer[75]. Infrastrukturen European Digital Credentials for Learning giver mulighed for at udstede digitalt underskrevne personlige kvalifikations- og mikroeksamensbeviser inden for cybersikkerhed. De indeholder detaljerede data, herunder om læringsresultater inden for cybersikkerhed, og de kan lagres i den fremtidige **digitale EU-dækkende eID-tegnebog**[76].

Tiltag under akademiet

Medlemsstaterne og industrien

- Sikre støtte til udvikling og anerkendelse af **mikroeksamensbeviser** for undervisning inden for cybersikkerhed i overensstemmelse med Rådets henstilling om en europæisk tilgang til mikroeksamensbeviser.
- Medtage cybersikkerhedskvalifikationer, herunder mikroeksamensbeviser, i de **nationale referencerammer for kvalifikationer**.
- Skabe **muligheder for læring på arbejdspladsen** gennem læringsforløb for personer, der deltager i initiativer til udvikling af cybersikkerhedsfærdigheder.

Kommissionen

- På kort sigt etablere **et fælles kontaktpunkt** for cybersikkerhedsprogrammer, eksisterende kurser og cybersikkerhedscertificeringer via **platformen for digitale færdigheder og job** inden udgangen af 2023.
- Foreslå en ændring af **forordningen om cybersikkerhed** for at gøre det muligt at certificere forvaltede sikkerhedsudbydere den 18. april 2023.

EU-organer og -agenturer

- Etablere **ECSF** som en fælles tilgang vedrørende rolleprofiler inden for cybersikkerhed og dertil knyttede færdigheder inden udgangen af 2023.
- ENISA skal igangsætte udviklingen af et pilotprojekt om oprettelse af en **europæisk attesteringsordning** for cybersikkerhedskompetencer i andet kvartal 2023.
- ENISA skal gennemgå **kursuskataloget** og tilbyde **"train the trainer"-programmet** til kritiske offentlige og private operatører inden udgangen af 2023.
- Afslutte **tilpasningen af ESDC's læseplaner til ECSF** inden midten af 2023.

5. Inddragelse af interessenter: forpligtelse til at afhjælpe manglen på cybersikkerhedskompetencer

[74] Rådets henstilling om en europæisk tilgang til mikroeksamensbeviser for livslang læring og beskæftigelsesegnethed

[75] Rådets henstilling af 22. maj 2017 om den europæiske referenceramme for kvalifikationer for livslang læring og om ophævelse af Europa-Parlamentets og Rådets henstilling af 23. april 2008 om etablering af den europæiske referenceramme for kvalifikationer for livslang læring

[76] Forslag til Europa-Parlamentets og Rådets forordning om ændring af forordning (EU) nr. 910/2014 for så vidt angår fastlæggelse af en ramme for en europæisk digital identitet

Under akademiet udvikles en koordineret tilgang til inddragelse af interessenter for at afhjælpe manglen på cybersikkerhedskompetencer. Målet er at maksimere synligheden og virkningen af de forskellige interessenters tilsagn om at mindske manglen på cybersikkerhedskompetencer.

Kommissionen opfordrer interessenterne til at give konkrete tilsagn om at opkvalificere og omskole arbejdstagere gennem målrettede foranstaltninger, der så vidt muligt afhjælper den konstaterede mangel på cybersikkerhedskompetencer. Sådanne **tilsagn fra interessenterne på cybersikkerhedsområdet** bør indberettes via **platformen for digitale færdigheder og job** i lighed med andre digitale tilsagn, der allerede er dokumenteret via platformen. Kommissionen opfordrer endvidere interessenterne til at give et tilsagn vedrørende cybersikkerhed via platformen og tilslutte sig **Digital Large Scale Partnership under pagten for færdigheder**[77]. Forpligtelserne på området for cybersikkerhed under Digital Large Scale Partnership bør dokumenteres via platformen for digitale færdigheder og job. På samme måde bør forpligtelser indgået inden for rammerne af platformen for digitale færdigheder og job indberettes under Digital Large Scale Partnership under pagten for færdigheder.

Kommissionen opfordrer endvidere medlemsstaterne til at **videreføre indsatsen for at gennemføre erklæringen Women in Digital**[78] for 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. Kommissionen opfordrer også medlemsstaterne til at udvikle synergier med programmerne under **Den Europæiske Socialfond+ (ESF+)** for yderligere at støtte målsætningen om ligestilling mellem kønnene i deltagelsen på arbejdsmarkedet[79], f.eks. ved at etablere **mentorprogrammer for piger og kvinder**. Det kan fremme etableringen af rollemodeller for at tiltrække piger til jobtyper inden for cybersikkerhed og samtidig bidrage til at nedbryde kønsstereotyper. Samtidig tilskyndes kvinder til at deltage i opkvalificering og omskoling, hvilket bidrager til udviklingen af et fællesskab, som støtter kvinders deltagelse og forfremmelse på jobmarkedet for cybersikkerhed.

Medlemsstaterne bør som led i **de nationale cybersikkerhedsstrategier vedtage specifikke foranstaltninger til at afhjælpe manglen på cybersikkerhedskvalifikationer**[80], identificere og forbedre formidlingsindsatsen for at afhjælpe kvalifikationsmanglen og derigennem sikre korrekt gennemførelse af forpligtelserne i henhold til NIS2-direktivet.

Nogle medlemsstater udnytter **synergier mellem** initiativer vedrørende **civilsamfund, forsvar og retshåndhævelse**. Det kan f.eks. være ved at øge arbejdsstyrken ved at gøre brug af værnepligtige eller reserver med speciale i cybersikkerhed, dvs. militæruddannede borgere i cybersikkerhedsjobs i de væbnede styrker[81] og gøre det muligt for befolkningen, og navnlig unge, at øge deres færdigheder inden for cybersikkerhed og cyberforsvar. Det samme gælder inden for **bekæmpelse af cyberkriminalitet**, da der er mange ligheder mellem den generelle cybersikkerhedsindsats og retshåndhævelsesaktiviteter som reaktion på

[77] Nye europæiske partnerskaber iværksat for at opfylde EU's ambitioner for det digitale årti | Europas digitale fremtid i støbeskeen (europa.eu), udarbejdet i forbindelse med pagten for færdigheder for at afhjælpe manglen på kompetencer inden for informations- og kommunikationsteknologi (IKT)

[78] EU countries commit to boost participation of women in digital | Europas digitale fremtid i støbeskeen (europa.eu).

[79] Europa-Parlamentets og Rådets forordning (EU) 2021/1057 af 24. juni 2021 om oprettelse af Den Europæiske Socialfond Plus (ESF+) og om ophævelse af forordning (EU) nr. 1296/2013, artikel 4, stk. 1, litra c)

[80] NIS2-direktivet, artikel 7, stk. 2, litra f)

[81] Report - Cyber Conscription: Experience and Best Practice from Selected Countries, Martin Hurt and Tiia Sõmer, International Centre for Defence and Security, februar 2021

cybersikkerhedshændelser. Kommissionen tilskynder til drøftelser blandt medlemsstaterne om sådanne initiativer og opfordrer dem til at vurdere, hvordan en kvalificeret arbejdsstyrke bedst kan tjene både forsvaret og civilsamfundet, når det gælder cybersikkerhed.

Kommissionen vil i gennemgangen af behovene i EU's institutioner, organer, kontorer og agenturer overveje forslag til, hvordan både nuværende og fremtidige identificerede mangler kan afhjælpes. Navnlig vil Kommissionen tilskynde personalet til at udnytte det kommende EU-USA cybersikkerhedsstipendium, der er etableret inden for rammerne af dialogen mellem EU og USA.

Tiltag under akademiet

Erhvervet

- Foreslå specifikke **cybersikkerhedsforpligtelser** via platformen for digitale færdigheder og job pr. 18. april 2023.

Medlemsstater

- Medtage specifikke foranstaltninger til at afhjælpe manglen på færdigheder inden for cybersikkerhed i de nationale cybersikkerhedsstrategier.

Medlemsstaterne og industrien

- Gennemføre erklæringen Women in Digital og sikre kønsmæssig konvergens i jobs inden for cybersikkerhed senest i 2030.

6. Finansiering: skabe synergier for at maksimere virkningen af udgifterne til udvikling af cybersikkerhedsfærdigheder

Under akademiet vil effekten af investeringer i cybersikkerhedsfærdigheder blive maksimeret ved at skabe et fælles kontaktpunkt, fremme en bedre fordeling af midlerne efter markedets behov og mainstreame anvendelsen af finansiering, fremme synergier mellem forskellige instrumenter og samtidig undgå dobbeltarbejde[82].

6.1. Tilpasning af midlerne til behovene

Under akademiet vil ECCC med støtte fra Kommissionen, ECCO-projektet og de nationale koordinationscentre indsamle **information om, hvordan EU-midlerne anvendes til finansiering af cybersikkerhedsfærdigheder**, og derudover vurdere, hvordan EU-midlerne afhjælper manglen på cybersikkerhedskompetencer. Under hensyntagen til den indsamlede information vil ECCC søge at sikre en bedre kanalisering af EU-midlerne i forhold til de identificerede behov. ECCC vil finansiere foranstaltninger, der afhjælper de mest presserende mangler i arbejdsstyrken inden for cybersikkerhed, herunder vedrørende gennemførelse af de cybersikkerhedspolitiske behov.

6.2. Synliggørelse af tilgængelige midler og partnerskabsinitiativer vedrørende cybersikkerhedsfærdigheder

[82] Finansieringsmuligheder (europa.eu) Pagten for støtte til færdigheder etablerer et fælles kontaktpunkt for information om finansiering af færdigheder, herunder for det digitale økosystem. Støttetjenesterne under pagten formidler generel information om finansieringsinstrumenter, der ikke specifikt er rettet mod cybersikkerhedsfærdigheder, men som akademiet uanset tjenesternes arbejde bør tage hensyn til for at undgå overlapning.

På kort sigt vil **platformen for digitale færdigheder og job** blive det centrale kontaktpunkt for interessenter, hvor alle oplysninger om finansieringsmuligheder for cybersikkerhedsfærdigheder vil være tilgængelige.

EU investerer i mennesker og deres færdigheder og anvender navnlig partnerskaber med industrien til at mobilisere tiltag vedrørende opkvalificering og omskoling gennem flere instrumenter, der er udpeget under den **europæiske dagsorden for færdigheder**[83], især **pagten for færdigheder**[84] og **handlingsplanen for digital uddannelse**[85]. **Programmet for et digitalt Europa** finansierer udvikling af cybersikkerhedsfærdigheder, navnlig gennem tværnationale projektinitiativer, og supplerer den støtte, som Horisont Europa yder til forskning og innovative teknologiske løsninger inden for cybersikkerhed. Den **Europæiske Forsvarsfond**[86] finansierer forskning og teknologisk udvikling med henblik på at gennemføre effektive cyberoperationer, herunder uddannelse og øvelser[87]. **Erasmus+** støtter fortsat sådanne initiativer, herunder gennem blandede intensive programmer og samarbejdsprojekter.

Medlemsstaterne opfordres til at mobilisere deres direkte forvaltede EU-midler til støtte for cybersikkerhedskvalifikationer og jobs inden for området. Samhørighedspolitikkens fonde, såsom **Den Europæiske Fond for Regionaludvikling (EFRU)** og **ESF+**, giver store muligheder for at skabe synergi i denne sammenhæng[88]. Foranstaltningerne under **genopretnings- og resiliensfaciliteten**[89] og **InvestEU**[90] giver mulighed for yderligere vigtig komplementaritet med hensyn til at opfylde akademiets mål.

Tiltag under akademiet

Det Europæiske Kompetencecenter for Cybersikkerhed og ENISA

- **Kortlægge** eksisterende EU-finansiering til cybersikkerhedsfærdigheder i forhold til markedsbehovene, vurdere **effektiviteten** og fastlægge **finansieringsprioriteter** inden udgangen af 2024.

Kommissionen

- Etablere et **fælles kontaktpunkt** for finansieringsmuligheder inden for cybersikkerhedsfærdigheder via platformen for digitale færdigheder og job inden udgangen

[83] Den europæiske dagsorden for færdigheder — Beskæftigelse, sociale anliggender, arbejdsmarkedsforhold og inklusion — Europa-Kommissionen (europa.eu)

[84] EU-finansieringsinstrumenter for opkvalificering og omskoling — Beskæftigelse, Sociale Anliggender, Arbejdsmarkedsforhold og Inklusion — Europa-Kommissionen (europa.eu)

[85] Handlingsplan for digital uddannelse 2021-2027

[86] Europa-Parlamentets og Rådets forordning (EU) 2021/697 af 29. april 2021 om oprettelse af Den Europæiske Forsvarsfond og om ophævelse af forordning (EU) 2018/1092

[87] Medlemsstaterne har forpligtet sig til fælles uddannelser og kurser, f.eks. ved at etablere og deltage i cyberuddannelse og -kurser under det permanente strukturerede samarbejde (PESCO) såsom EU's cyberakademi og -innovationsknudepunkt (EU CAIH) og Federated Cyber Ranges.

[88] Forordning (EU) 2021/1058 artikel 3, stk. 1, og forordning (EU) 2021/1057, artikel 4, stk. 1, litra g).

[89] For eksempel omfatter den estiske genopretnings- og resiliensplan investeringer (10 mio. EUR) i digitale færdigheder, der omfatter revision af de kurser, der tilbydes IKT-eksperter, finansiering af opkvalificering og omskoling af IKT-specialister inden for cybersikkerhed og bidrag til udviklingen af et pilotprogram med henblik på at ændre kvalifikationsrammen for IKT-specialister.

[90] Interessenter (f.eks. uddannelsesudbydere og virksomheder, der ønsker at udforme eller forbedre uddannelsesaktiviteter inden for cybersikkerhed) kan henvende sig til InvestEU-rådgivningsplatformen, der yder teknisk støtte og bistand, herunder kapacitetsopbygning, til projektudviklere og enheder, og konsultere InvestEU-portalen.

af 2023.

7. Måling af fremskridt: indbygget ansvarlighed

Under akademiet udvikles en **metode** til at **måle fremskridtene med hensyn til at afhjælpe manglen på cybersikkerhedskompetencer**.

7.1. Definition af cybersikkerhedsindikatorer til overvågning af udviklingen på arbejdsmarkedet for cybersikkerhed

Indekset over den digitale økonomi og det digitale samfund (DESI) opsummerer indikatorer for Europas digitale resultater og følger udviklingen i EU's medlemsstater. Under akademiet for cybersikkerhedskompetencer udvikler ENISA i samarbejde med Kommissionen og NIS-samarbejdsgruppen[91] **indikatorer**, herunder for kønsfordeling, for at følge udviklingen i EU's medlemsstater med hensyn til at øge antallet af cybersikkerhedseksperter, og hører i den sammenhæng de relevante markedsaktører og de nationale koordinationscentre. ENISA benytter DESI-metoden[92] og sikrer, at indikatorerne er i overensstemmelse med Europas digitale mål for IKT-fagfolk og for opnåelse af kønsmæssig konvergens inden for IKT. Kommissionen sikrer derefter integration af indikatorerne i DESI, så det bliver muligt år for år at gøre status over situationen vedrørende cybersikkerhedsfærdigheder og jobmarkedet.

7.2. Dataindsamling og rapportering

ENISA indsamler data om indikatorerne med støtte fra ECCO-projektet og de nationale koordinationscentre. Baseret på de indsamlede data udarbejder ENISA en **årlig rapport**, der kan indgå i statusrapporten om det digitale årti[93], som sammen med DESI desuden indgår i de landespecifikke analyser og anbefalinger, der udarbejdes under det europæiske semester[94]. Desuden bidrager indikatorerne for cybersikkerhedsfærdigheder til ENISAs **toårsrapport** om cybersikkerhedssituationen i EU, der er fastsat i NIS2-direktivet, og som dækker cybersikkerhedskapaciteten, cyberbevidstheden og cyberhygiejnen i hele EU.

7.3. Udarbejdelse af centrale resultatindikatorer (KPI'er) for cybersikkerhed

Med henblik på at afhjælpe manglen på cybersikkerhedskompetencer i Europa vil ENISA i tæt samarbejde med Kommissionen og de nationale koordinationscentre foreslå KPI'er til Kommissionen på grundlag af metodologien fra politikprogrammet for det digitale årti 2030 samt industriens erfaringer. ENISA tager behørigt højde for de KPI'er, som medlemsstaterne anvender til at vurdere de nationale cybersikkerhedsstrategier[95].

Tiltag under akademiet

ENISA

[91] Gennem brug og udbygning af den metode, der skal udvikles af ENISA til brug for agenturets toårsrapport om cybersikkerhedssituationen i Unionen i henhold til artikel 18, stk. 3, i NIS 2-direktivet.

[92] Se metodenote 2022 fra indekset for den digitale økonomi og det digitale samfund (DESI) her The Digital Economy and Society Index (DESI) | Shaping Europe's digital future (europa.eu).

[93] Europa-Parlamentets og Rådets afgørelse (EU) 2022/2481 af 14. december 2022 om etablering af politikprogrammet for det digitale årti 2030

[94] Ibidem, betragtning 25

[95] NIS2-direktivet, artikel 7, stk. 4

- Udarbejde **indikatorer og KPI'er** for cybersikkerhedsfærdigheder inden udgangen af 2023.
- **Indsamle data** om indikatorer og rapportere herom med første dataindsamling senest i 2025.

Kommissionen

- Bidrage til integration af **indikatorer for cybersikkerhed i DESI** og i **rapporten om det digitale årti**.

8. Konklusion

Denne meddelelse danner grundlag for en modernisering af EU's tilgang til at øge færdighederne inden for cybersikkerhed for fagfolk i EU. Målet er at reducere manglen på cybersikkerhedskompetencer og sikre EU den nødvendige arbejdsstyrke, så EU kan håndtere et trusselsbillede i konstant forandring, gennemføre EU-politikker, der har til formål at beskytte EU mod cyberangreb, og styrke forretningsmulighederne og konkurrenceevnen. En kvalificeret arbejdsstyrke inden for cybersikkerhed vil være til gavn for **civilsamfund, forsvar, diplomati og retshåndhævelse** og fremme synergier herimellem.

Kommissionen opfordrer medlemsstaterne og alle interessenter til at bidrage til at opfylde målsætningerne for akademiet for cybersikkerhedskompetencer.