EUROPEISKA
KOMMISSIONEN

Strasbourg den 18.4.2023
COM(2023) 207 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens
(*EU-akademin för cyberkompetens*)

Minska kompetensbristen på cybersäkerhetsområdet för att främja EU:s konkurrenskraft, tillväxt och resiliens (*EU-akademin för cyberkompetens*)

1. Ett akut behov av att minska riskerna genom att komma till rätta med kompetensbristen på cybersäkerhetsområdet

Cybersäkerheten är inte bara en del av medborgarnas, företagens och medlemsstaternas säkerhet. Den är också nödvändig för att säkerställa EU:s politiska stabilitet, stabiliteten i dess demokratier och vårt samhälles och våra företags välstånd. **Hotbilden** på cybersäkerhetsområdet har förändrats kraftigt de senaste åren och en oroande trend är att allt fler cyberattacker riktar sig mot militär och civil kritisk infrastruktur i EU. Fientliga aktörer får allt större kapacitet och det dyker upp nya hot, hybridhot och framväxande hot, såsom användningen av bottar och teknik som bygger på artificiell intelligens[1]. I synnerhet orsakar fientliga aktörer som använder sig av utpressningsprogram företagen rutinmässigt stora skador, både ekonomiskt och i förlorat anseende[2].

Ett stort antal cybersäkerhetsincidenter har också varit riktade mot offentlig förvaltning och regeringar i medlemsstaterna samt mot EU:s institutioner, organ och byråer[3]. Finanssektorn[4] och hälso- och sjukvårdssektorn[5], som båda utgör samhällets och ekonomins ryggrad, har också konsekvent varit föremål för incidenter[6]. De geopolitiska spänningarna till följd av Rysslands anfallskrig mot Ukraina har ökat cybersäkerhetshotet[7] och riskerar att destabilisera vårt samhälle. EU:s **säkerhet** kan inte garanteras utan **EU:s mest värdefulla tillgång: människorna.** EU har ett akut behov av yrkesverksamma personer med färdigheter och kompetens att förebygga, upptäcka, avskräcka och försvara EU, inbegripet dess mest kritiska infrastruktur, mot cyberattacker och säkerställa dess **resiliens**.

Kompetensbristen på cybersäkerhetsområdet hämmar också Europas **konkurrenskraft** och **tillväxt**, som i hög grad är beroende av utvecklingen och användningen av strategisk digital teknik (t.ex. artificiell intelligens, 5G och molntjänster). Det behövs kvalificerad arbetskraft inom cybersäkerhet för att EU ska kunna fortsätta att tillhandahålla viktig avancerad teknik i en global miljö.

---

[1] Enisas hotbildsrapport 2022 – Enisa (europa.eu).

[2] Europols hotbildsbedömning av internetstödd organiserad brottslighet (Iocta) 2021. Dessa aktörer bygger på modellen utpressningsprogram som tjänst. Företagens årliga kostnad uppgick till över 18,4 miljarder euro 2022 (Cybereasons rapport från 2022 om de faktiska kostnaderna för utpressningsprogrammen).

[3] Se till exempel Enisas och CERT-EU:s gemensamma publikation *JP-23–01 – Sustained activity by specific threat actors*, TLP:CLEAR, av den 15 februari 2023.

[4] I Tyskland utgjorde till exempel 90 % av de rapporterade e-postbedrägerierna från den 1 juni 2021 till den 31 maj 2022 finansrelaterat nätfiske, och en attack mot ett företag inom finanssektorn omfattade mer än 20 000 smittade enheter från 125 länder. Se *The State of IT Security in Germany 2022*, Bundesamt für Sicherheit in der Informationstechnik (BSI), av den 1 januari 2023.

[5] I Frankrike utsattes till exempel offentliga vårdinrättningar, t.ex. Centre Hospitalier Sud Francilien, för utpressningsattacker, där en fientlig aktör röjde och publicerade 11 GB personuppgifter och medicinska uppgifter samt personalrelaterade uppgifter. Se *Panorama de la cybermenace 2022*, Agence nationale de la sécurité des systèmes d'information (ANSSI), januari 2023.

[6] Enisas hotbildsrapport 2022.

[7] Se även CERT-EU – Russia's war on Ukraine: one year of cyber operations (europa.eu), *Ryska cyberoperationer mot Ukraina: uttalande av EU:s utrikesrepresentant på EU:s vägnar*, av den 10 maj 2022, *Uttalande av EU:s utrikesrepresentant om skadlig cyberverksamhet som utförs av hackare och hackargrupper inom ramen för Rysslands angrepp mot Ukraina*, av den 19 juli 2022.

För att ha beredskap för och kunna hantera denna föränderliga hotbild och främja EU:s konkurrenskraft har EU:s cybersäkerhetspolitik gjort betydande framsteg under de senaste åren. Detta har lett till att det har antagits ett antal initiativ, såsom EU:s strategi för cybersäkerhet för ett digitalt decennium[8], det reviderade direktivet om säkerhet i nätverks- och informationssystem (NIS 2-direktivet)[9], EU:s sektorslagstiftning för cybersäkerhet[10], EU:s politik för cyberförsvar[11], och det förslag till cybersolidaritetsakt[12] som kommissionen lägger fram tillsammans med detta meddelande. Men utan den kvalificerade personal som behövs för att genomföra dem kommer målen med dessa rättsakter inte att nås. Även om allmänhetens grundläggande kunskaper i cybersäkerhet är en fråga som hanteras inom ramen för de initiativ som ska stödja utvecklingen av de allmänna färdigheter som behövs för att delta i samhället[13] är en kompetent arbetsstyrka avgörande,, både inom den offentliga och den privata sektorn, på nationell nivå och EU-nivå, inbegripet i standardiseringsorganisationer, **för att uppfylla dessa rättsliga och politiska krav på cybersäkerhet**.

EU:s säkerhet och konkurrenskraft är därför beroende av att ha en kvalificerad arbetsstyrka inom cybersäkerhet. EU står dock inför en mycket stor brist på kvalificerad cybersäkerhetspersonal, vilket innebär att EU, dess medlemsstater, företag och medborgare riskerar att bli föremål för cybersäkerhetsincidenter. 2022 saknades **mellan 260 000**[14] **och 500 000**[15] yrkespersoner inom cybersäkerhet i EU, samtidigt som EU:s personalbehov på cybersäkerhetsområdet uppskattades till 883 000 personer[16], vilket tyder på en bristande överensstämmelse mellan den kompetens som finns och den som behövs på arbetsmarknaden. Arbetsstyrkan inom cybersäkerhet drabbas dessutom av missuppfattningen om dess tekniska image och den har fortfarande problem att locka till sig **kvinnor**, som utgör 20 % av de personer som utexamineras inom cybersäkerhet[17] och 19 % av de specialister som finns inom informations- och kommunikationsteknik (IKT)[18]. För att komma till rätta med detta har EU i sitt **policyprogram för det digitala decenniet 2030**[19] fastställt målet att utöka

[8] *Gemensamt meddelande till Europaparlamentet och rådet: EU:s strategi för cybersäkerhet för ett digitalt decennium*, JOIN/2020/18 final.

[9] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

[10] För finanssektorn till exempel Europaparlamentets och rådets förordning (EU) 2022/2554 av den 14 december 2022 om digital operativ motståndskraft för finanssektorn och om ändring av förordningarna (EG) nr 1060/2009, (EU) nr 648/2012, (EU) nr 600/2014, (EU) nr 909/2014 och (EU) 2016/1011 (DORA-förordningen).

[11] Gemensamt meddelande till Europaparlamentet och rådet, EU:s politik för cyberförsvar, JOIN(2022) 49 final.

[12] Förslag till Europaparlamentets och rådets förordning om övergripande cybersäkerhetskrav för produkter med digitala element och om ändring av förordning (EU) 2019/1020, COM(2022) 454 final.

[13] Några av dessa initiativ för att öka allmänhetens generella digitala färdigheter är målet att 80 % av befolkningen senast 2030 ska ha grundläggande digitala färdigheter i handlingsplanen för den europeiska pelaren för sociala rättigheter och den digitala kompassen, handlingsplanen för digital utbildning 2021–2027, verktyget för den digitala kompetensramen eller förslaget till rådets rekommendation om att förbättra utbudet av digitala färdigheter i utbildningen.

[14] (ISC)² i *Assessing Cyber Skills on the basis of the ECSF*, Enisa-webbinarium den 16 februari 2023.

[15] Enligt Europeiska cybersäkerhetsorganisationens (Ecso) uppgifter i det gemensamma meddelandet till Europaparlamentet och rådet, *EU:s politik för cyberförsvar*, JOIN(2022) 49 final.

[16] (ISC²) i *Assessing Cyber Skills on the basis of the ECSF*, Enisa-webbinarium den 16 februari 2023.

[17] Databasen Cybersecurity Higher Education Database (CyberHEAD).

[18] Endast 19 % av IKT-specialisterna i EU är kvinnor Index för digital ekonomi och digitalt samhälle (Desi) 2022 | Att forma EU:s digitala framtid (europa.eu). Det finns ingen uppgift om hur många kvinnor som arbetar med cybersäkerhet i unionen.

[19] Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030, genom vilket det fastställs en uppföljnings- och samarbetsmekanism för att nå de

arbetsstyrkan inom IKT med 20 miljoner personer fram till 2030 och samtidigt uppnå en jämnare könsfördelning. Dessutom kräver genomförandet av EU:s nya politik en tillräckligt kvalificerad och tillräckligt stor arbetsstyrka. Till exempel lyfte över 42 % av de högre it-cheferna inom sektorn för finansiella tjänster fram bristen på kompetens och expertis inom cybersäkerhet som en viktig utmaning för deras verksamhet när det gäller cyberförsvar och incidenthantering[20], vid en tidpunkt då de kommer att behöva genomföra sektorsspecifik cybersäkerhetslagstiftning såsom förordningen om digital operativ motståndskraft för finanssektorn (DORA).

Arbetsgivarna, som ogärna investerar i humankapital, utan hellre söker färdigutbildad och erfaren arbetskraft, bidrar också till att begränsa arbetsmarknaden[21]. Denna brist drabbar alla typer av företag, inklusive **små och medelstora företag**, som utgör 99 % av alla företag i EU[22]. Den innebär också stora svårigheter för **offentliga förvaltningar** som drabbas hårt och påverkas mest av cybersäkerhetsincidenter[23].

Det är därför angeläget att snarast minska EU:s kompetensbrist på cybersäkerhetsområdet, eftersom EU:s säkerhet och konkurrenskraft står på spel.

2. Bristen på synergier och samordnade åtgärder för att minska kompetensbristen på cybersäkerhetsområdet

Offentliga och privata aktörer har vidtagit en lång rad initiativ på såväl europeisk som nationell nivå för att komma till rätta med bristen på arbetskraft på cybersäkerhetsområdet. Dessa är dock spridda och har hittills inte nått en kritisk massa för att göra verklig skillnad.

Till att börja med finns det för närvarande en begränsad samsyn om sammansättningen av EU:s arbetsstyrka på cybersäkerhetsområdet och dess färdigheter, medan snarlika yrkesprofiler inom cybersäkerhet bör omfatta samma färdigheter. De berörda aktörernas låga användning av den gemensamma **europeiska referensramen för cybersäkerhetspersonal** innebär att det saknas ett kommunikationsverktyg mellan arbetsgivare, utbildare och beslutsfattare och att det inte går att mäta och bedöma de brister som finns på arbetsmarknaden för cybersäkerhet. Detta gör dessutom att det för dem som vill komma in i yrket inte utformas utbildningsplaner eller skapas karriärvägar som motsvarar de politiska behoven och marknadens behov. **Kompetensutveckling och omskolning** av arbetsstyrkan är i hög grad beroende av cybersäkerhetsutbildning och cybersäkerhetscertifikat som i regel tillhandahålls av privata leverantörer. Arbetsstyrkan har dock svårt att få en överblick över kvaliteten på den cybersäkerhetsutbildning som erbjuds och de tillhörande certifikat som utfärdas.

Medan utbildning och karriärvägar är nödvändiga för att förbättra arbetsmarknadens utbudssida underskattas i dag **efterfrågesidans** roll för utbildningen av arbetsstyrkan och anpassningen till dess utveckling är för närvarande underskattad. Privata och offentliga arbetsgivare saknar gemensamma forum och platser för att samla idéer om hur man bäst kan utbilda arbetsstyrkan och hur man bättre kan **bedöma färdigheter**, särskilt under rekryteringsprocessen. Även om de mest efterfrågade **hårda färdigheterna** är

---

gemensamma mål för Europas digitala omställning som fastställs i den digitala kompassen 2030, bland annat på kompetensområdet.

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

[21] *Cybersecurity Skills Development in the EU*, Enisa, december 2019.

[22] Definition av små och medelstora företag (europa.eu).

[23] Enisas hotbildsrapport 2022 – Enisa (europa.eu).

cybersäkerhetsrelaterade[24], såsom programvaruutveckling eller molntjänster[25], förbises **generella färdigheter** fortfarande i omotiverad utsträckning. Kritiskt tänkande och kritisk analys, problemlösning och *self-management* är kompetensområden som arbetsgivarna efterfrågar alltmer[26] och som blir allt viktigare fram till 2025[27].

Det finns redan många offentliga och privata investeringsinitiativ för att höja kompetensen inom cybersäkerhet, och EU **finansierar** en lång rad projekt inom olika instrument[28]. Den fortsatta bristen på kompetens i EU väcker dock frågor om deras synlighet och effekt och tyder på att de kanske inte systematiskt motsvarar marknadens behov, som snarast måste kartläggas på EU-nivå. Med flera finansieringskällor blir det också dubbelarbete, vilket innebär att man går miste om möjligheten att skala upp och åstadkomma verklig effekt. Dessutom kan de som behöver investeringen inte alltid fastställa vilka källor som är lämpligast för deras behov.

Olika aktörer har försökt att ta itu med den komplexa och mångfasetterade frågan om bristen på cybersäkerhetskompetens. Europeiska unionens cybersäkerhetsbyrå (Enisa) har utvecklat instrument för yrkesprofiler eller högre utbildning[29], Europeiska kompetenscentrumet för cybersäkerhet (ECCC)[30] arbetar med cybersäkerhetskompetens i en särskild arbetsgrupp, Europeiska säkerhets- och försvarsakademin (Esfa) arbetar med den civila och militära personalens cybersäkerhetskompetens inom ramen den gemensamma säkerhets- och försvarspolitiken[31], privata organisationer försöker angripa frågan[32], och branschen för cybersäkerhetscertifiering håller på att utarbeta en färdplan och utbildningar för att komma till rätta med kompetensbristen[33]. Medlemsstaterna försöker också att ta itu med frågan genom en rad olika initiativ, från lagstiftning[34] till inrättande av akademier för cyberkompetens[35] eller cybercampus[36], kompetenscentrum mot it-brottslighet[37] eller genom offentlig-privata partnerskap[38]. Ofta saknar alla dessa aktörers insatser dock samordning och synergier och de har inte lyckats göra någon betydande skillnad på arbetsmarknaden, vilket framgår av den ökande bristen på cybersäkerhetspersonal i EU. Det behövs också ökade synergier mellan olika cybergemenskaper eftersom den kompetens som krävs för att

---

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

[25] ISACA-infografik om cybersäkerheten 2022

[26] Till exempel Cedefops verktyg Skills-OVATE | Cedefop (europa.eu).

[27] *The Future of Jobs Report*, oktober 2020, Världsekonomiskt forum.

[28] Det handlar exempelvis om följande: Cybersecurity Skills Alliance – New Vision for Europe – REWIRE-projektet (finansieras genom Erasmus+-programmet), projekt till stöd för kompetenscentrumet för cybersäkerhet (Echo, Concordia, CyberSec4Europe, SPARTA (finansieras genom Horisont 2020), Cybersecpro-projektet (finansieras genom programmet för ett digitalt Europa).

[29] Till exempel den europeiska kompetensramen för cybersäkerhet (ECSF), Cyberhead – databasen för högre utbildning i cybersäkerhet, plattformen för cybersäkerhetsövningar (CEP), den europeiska cybersäkerhetsutmaningen, Europeiska månaden för cybersäkerhet.

[30] Europaparlamentets och rådets förordning (EU) 2021/887 av den 20 maj 2021 om inrättande av Europeiska kompetenscentrumet för cybersäkerhet inom näringsliv, teknik och forskning och av nätverket av nationella samordningscentrum.

[31] Till exempel plattformen för utbildning, träning, bedömning och övning (ETEE) på cyberområdet.

[32] Till exempel Europeiska cybersäkerhetsorganisationens (Ecso) arbetsgrupp 5 om utbildning, medvetenhet, cyberranger och mänskliga faktorer, organisationen DIGITALEUROPE .

[33] Till exempel SANS-institutet (ISC)², ISACA.

[34] Till exempel i nationella strategier för utbildning eller cybersäkerhet.

[35] Till exempel C-akademin i Portugal.

[36] Till exempel cybercampus i Frankrike.

[37] Till exempel Litauens kompetenscentrum mot it-brottslighet för forskning och utbildning i Litauen (L3CE).

[38] Till exempel Microsofts initiativ för cybersäkerhetsutbildning.

upprätthålla cybersäkerheten, bekämpa **it-brottsligheten** eller bygga upp **cyberförsvarsåtgärder** ofta är av liknande karaktär.

Slutligen har EU i dag begränsade möjligheter att bedöma **läget och utvecklingen på arbetsmarknaden för cybersäkerhet** och arbetsstyrkans kompetens. Medlemsstaterna och EU:s institutioner, organ och byråer förlitar sig antingen på uppgifter som samlats in av privata företag eller på en bredare uppsättning uppgifter om IKT-personal som samlats in av EU, framförallt av Eurostat[39] och Europeiskt centrum för utveckling av yrkesutbildning (Cedefop)[40]. EU har med andra ord en ofullständig och fragmenterad bild av sina behov, vilket hindrar unionen från att konsolidera en samlad vision om läget på arbetsmarknaden för cybersäkerhet.

3. En samordnad strategi för hela EU: EU-akademin för cyberkompetens

3.1.Målet

För att klara utmaningen att höja cybersäkerhetskompetensen och minska bristen på arbetsmarknaden föreslår kommissionen en **EU-akademi för cyberkompetens**, som Europeiska kommissionens ordförande tillkännagav i sin avsiktsförklaring om tillståndet i unionen 2022[41, , 42]och i samband med Europaåret för kompetens.

Syftet med EU-akademin för cyberkompetens (nedan kallad *akademin*) är att skapa en **gemensam kontaktpunkt och synergier** för erbjudanden om cybersäkerhetsutbildning samt för finansieringsmöjligheter och särskilda åtgärder för att stödja kompetensutvecklingen inom cybersäkerhet. Den kommer att skala upp de olika aktörernas initiativ för att uppnå en kritisk massa som kommer att göra skillnad på arbetsmarknaden, även på försvarsområdet. Dessa verksamheter skulle anpassas efter gemensamma mål och centrala resultatindikatorer för att uppnå större genomslag.

Akademin kommer att fokusera på utbildning av **yrkespersoner inom cybersäkerhet**. Akademins verksamhet kommer att bidra till EU:s cybersäkerhetspolitik, men också till utbildning och livslångt lärande. Den kompletterar de två rådsrekommendationer om digital utbildning och digitala färdigheter som kommissionen föreslagit samtidigt som detta meddelande[43].

Akademin kommer att bygga på fyra pelare: 1. **Genom utbildning främja kunskapsutvecklingen** genom att arbeta med en gemensam ram för yrkesprofiler inom cybersäkerhet och tillhörande färdigheter, förbättra det europeiska utbildningsutbudet för att tillgodose behoven, skapa karriärvägar och skapa synlighet och tydlighet när det gäller cybersäkerhetsutbildning och certifiering för att förbättra arbetskraftens utbudssida. 2. Säkerställa en bättre kanalisering av och överblick över tillgängliga **finansieringsmöjligheter** för kompetensrelaterad verksamhet för att maximera deras effekt. 3. Uppmana berörda parter **att vidta åtgärder**. 4. Fastställa indikatorer för att **övervaka marknadsutvecklingen** och kunna bedöma åtgärdernas ändamålsenlighet.

---

[39] Sysselsättning för IKT-specialister – Statistics Explained (europa.eu).

[40] Till exempel Cedefops verktyg Skills-OVATE | Cedefop (europa.eu).

[41] 2022 års avsiktsförklaring om tillståndet i unionen till talman Roberta Metsola och premiärminister Petr Fiala.

[42] Gemensamt meddelande till Europaparlamentet och rådet, *EU:s politik för cyberförsvar*, JOIN(2022) 49 final.

[43]Förslag till rådets rekommendationer om de viktigaste möjliggörande faktorerna för framgångsrik digital utbildning och om att förbättra utbudet av digitala färdigheter i utbildningen.

Genomförandet av akademin kommer att stödjas med 10 miljoner euro från programmet för ett digitalt Europa[44].

3.2.Akademins styrning

För att tillhandahålla en infrastruktur som fungerar som **en gemensam kontaktpunkt** för att främja samarbete mellan den akademiska världen, utbildningsanordnare och näringslivet, där utbuds- och efterfrågesidorna i EU:s cybersäkerhetsekosystem kan mötas och utbildas, skulle akademin kunna ta formen av ett **europeiskt konsortium för digital infrastruktur (Edic)**[45]. Detta instrument skulle göra det möjligt för medlemsstaterna att tillsammans arbeta för att minska kompetensbristen inom cybersäkerhet och att nära samarbeta med kommissionen, Enisa och Europeiska kompetenscentrumet för cybersäkerhet (ECCC), i enlighet med deras mandat och kompetens, och att involvera alla berörda parter, men även styra europeiska, nationella och privata investeringar mot ett gemensamt mål. Därför uppmanas intresserade medlemsstater att senast den 30 maj 2023 lämna in en förhandsanmälan till kommissionen av deras framtida ansökan till ett sådant Edic-konsortium. Denna frivilliga förhandsanmälan skulle göra det möjligt för kommissionen att tidigt lämna synpunkter på utkastet till Edic-ansökan, och på så sätt göra det möjligt att vidareutveckla och formellt lämna in den på ett snabbare sätt. Kommissionen kommer under hela processen och i den utsträckning medlemsstaterna begär det att fungera som en projektaccelerator för flera länder och på så sätt underlätta utarbetandet av Edic-ansökan. Därefter, när ansökan fått en positiv bedömning av kommissionen och godkänts av kommittén för policyprogrammet för det digitala decenniet, kommer kommissionen att fatta ett beslut om inrättande av Edic-konsortiet och därefter hjälpa till att samordna konsortiets genomförande[46].

Under tiden, och medan Edic-konsortiet formellt håller på att inrättas, kommer kommissionen att inrätta en virtuell gemensam kontaktpunkt genom att stärka kommissionens **plattform för digital kompetens och digitala arbetstillfällen**[47] med stöd av projektet European Cybersecurity Community Support (ECCO)[48].

Enisa kommer att bidra till genomförandet av akademin i enlighet med byråns mål[49], särskilt när det gäller stöd till cybersäkerhetsutbildning, och med beaktande av dess rapporteringsskyldigheter enligt NIS 2-direktivet[50]. **ECCC** kommer att arbeta i enlighet med sin strategiska agenda för att stödja genomförandet av EU-akademin för cyberkompetens. ECCC kommer framför allt att genomföra strategiskt mål 3 (cybersäkerhet) i programmet för ett digitalt Europa. Det kommer att få stöd från kommissionen och medlemsstaterna genom de **nationella samordningscentrumen**. Den **samarbetsgrupp** som inrättats enligt NIS 2-

---

[44] Europaparlamentets och rådets förordning (EU) 2021/694 av den 29 april 2021 om inrättande av programmet för ett digitalt Europa och om upphävande av beslut (EU) 2015/2240.

[45] Edic-konsortierna inrättades genom Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030, artikel 13 och följande artiklar.

[46] Ibid, artikel 12.

[47] Hem | Plattformen för digital kompetens och digitala arbetstillfällen (europa.eu).

[48] Se Europeiska kompetenscentrumet för cybersäkerhet och dess nätverk: nytt EU-finansierat projekt för att stödja cybergemenskapen (europa.eu). I december 2022 undertecknade Europeiska kommissionen ett kontrakt på 3 miljoner euro för att stödja EU:s cybergemenskap inom ramen för Europeiska kompetenscentrumet för cybersäkerhet. Detta projekt kommer att bidra till EU:s mål om samhälls- och kapacitetsuppbyggnad när det gäller forskning, innovation, användning och industriell bas inom cybersäkerhet.

[49] ”Enisa ska stödja kapacitetsuppbyggnad och beredskap i hela unionen genom att bistå unionens institutioner, organ och byråer, liksom medlemsstaterna och offentliga och privata intressenter i syfte att [...] utveckla färdigheter och kompetens inom området cybersäkerhet.” Artikel 4.3 i förordningen om cybersäkerhet.

[50] Artikel 18 i NIS 2-direktivet.

direktivet[51] kommer att tillkallas när det är lämpligt. Slutligen kommer samarbete med **näringslivet** och **den akademiska världen** att vara en förutsättning för att nå akademins mål att minska kompetensbristen inom cybersäkerhet.

4. Kunskapsutveckling och utbildning: fastställa en gemensam EU-strategi för cybersäkerhetsutbildning

Inom ramen för akademins pelare för kunskapsutveckling och utbildning kommer en strukturerad strategi att utvecklas med det tydliga målet att utöka **antalet** personer med cybersäkerhetskompetens i EU, bättre anpassa utbildningen efter **marknadens behov** och synliggöra **karriärvägar**.

4.1. Att tala samma språk: en gemensam strategi för yrkesprofiler inom cybersäkerhet och tillhörande färdigheter

Enisa har redan inlett arbetet med att fastställa yrkesprofiler för personer som arbetar med cybersäkerhet inom ramen för den **europeiska kompetensramen för cybersäkerhet**[52]. Akademin bör utgå från dessa för att fastställa och bedöma relevanta färdigheter, övervaka kompetensbristens utveckling och ta fram indikationer för de nya behoven. För varje cybersäkerhetsroll i kompetensramen ingår en uppsättning tillämpliga europeiska e-kompetensramar[53] som en del av profilbeskrivningen[54].

Enisa kommer därför att se över den europeiska kompetensramen för cybersäkerhet och **identifiera framväxande kompetensbehov och kompetensbrister** i arbetsstyrkan inom cybersäkerhet, bland annat med hjälp av avancerade verktyg (t.ex. artificiell intelligens, stordata[55], datautvinning). Därför kommer Enisa att arbeta under ledning av Edic-konsortiet, när det har inrättats, ECCC, tillsammans med nationella samordningscentrum, kommissionen, ECCO-projektet och marknadsaktörer[56]. När det gäller arbetsstyrkan inom cyberförsvar kommer Enisa att ta vederbörlig hänsyn till Esfas arbete. På samma sätt kommer Enisa, när det gäller att bekämpa it-brottslighet, att ta hänsyn till det arbete som bedrivs av Europeiska unionens byrå för utbildning av tjänstemän inom brottsbekämpning (Cepol) och Europol för att inrätta en operativ behovsanalys[57] för cyberattacker.

Den europeiska kompetensramen för cybersäkerhet kommer under akademins ledning att regelbundet kompletteras och ses över under en tvåårscykel. Dessutom kommer kommissionen och Europeiska utrikestjänsten att bidra till att fastställa specifika profiler och

---

[51] Europaparlamentets och rådets direktiv (EU) 2022/2555 av den 14 december 2022 om åtgärder för en hög gemensam cybersäkerhetsnivå i hela unionen, om ändring av förordning (EU) nr 910/2014 och direktiv (EU) 2018/1972, och om upphävande av direktiv (EU) 2016/1148 (NIS 2-direktivet).

[52] Den europeiska kompetensramen för cybersäkerhet – Enisa (europa.eu). Europeiska kompetensramen gör det lättare att identifiera och utforma uppgifter, kompetenser, färdigheter och kunskaper som rör den europeiska cybersäkerhetspersonalens yrkesroller. Den sammanfattar alla cybersäkerhetsrelaterade roller i profiler, som analyseras var för sig i detalj inom deras respektive ansvarsområden, färdigheter, synergier och ömsesidiga beroenden.

[53] Den europeiska ramen för e-kompetens | Esco (europa.eu). Den europeiska ramen för e-kompetens skapar konsekventa förbindelser när det gäller IKT-kvalifikationer och andra ramar som är relevanta för sektorn, däribland DigComp.

[54] Se i detta avseende *User Manual – European Cybersecurity Skills Framework (ECSF)* – september 2022.

[55] Se till exempel Skills-OVATE som utvecklats av Cedefop.

[56] Byrån kommer att ytterligare utnyttja resultaten från andra EU-finansierade projekt (t.ex. Rewire, det gemensamma europeiska dataområdet för kompetens (DS4S), CyberSecPro och Concordia) och metoder som härrör från liknande initiativ (t.ex. OECD-rapporten *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States* som lades fram den 21 mars 2023) för att i framtiden säkerställa en uppdaterad vision av behoven i en miljö där efterfrågan ständigt utvecklas.

[57] Cepols analys av det operativa utbildningsbehovet.

tillhörande färdigheter för olika sektorer efter behov, med stöd av EU:s byråer och organ, såsom Esfa[58], Europol och Cepol[59].

Förbindelser kommer också att upprättas mellan den europeiska kompetensramen för cybersäkerhet och relevanta instrument inom EU:s sysselsättningspolitik[60]. I synnerhet kommer kompetensramens yrkesprofiler och tillhörande färdigheter att integreras i **Esco-klassificeringen**. Detta kommer att förbättra klassificeringen av och kopplingarna mellan yrken och färdigheter på cybersäkerhetsområdet, vilket gör det lättare för människor att vidareutbilda och omskola sig och stöder kompetensbaserad jobbmatchning och gränsöverskridande rörlighet.

4.2.Främja samarbete för att utforma läroplaner för cybersäkerhetsutbildning

När Edic-konsortierna har inrättats bör medlemsstaterna hjälpa akademin att bli **Europas referensplats för utformning och tillhandahållande av cybersäkerhetsutbildningar** i de mest efterfrågade färdigheterna. Akademin bör erbjuda nystartade företag och små och medelstora företag samt offentliga förvaltningar arbetsplatsanknuten utbildning och praktikmöjligheter på innovativa företag inom cybersäkerhet och kompetenscentrum för cybersäkerhet. Edic-konsortiet bör samarbeta med alla berörda parter, inbegripet näringslivet, för att utforma sådana utbildningar. De bör bygga vidare på projekt som **CyberSecPro**[61], som finansieras av programmet för ett digitalt Europa och som består av 17 högre utbildningsanstalter och 13 säkerhetsföretag från 16 medlemsstater, som tillsammans vill skapa bästa praxis för alla utbildningsprogram inom cybersäkerhet.

Akademin kommer att samarbeta med alla berörda parter för att **locka de unga generationerna** till en karriär inom cybersäkerhet. I enlighet med förslaget till rådets rekommendation om att förbättra utbudet av digitala färdigheter i utbildningen bör medlemsstaterna införa och stärka åtgärder för att rekrytera och utbilda specialiserade lärare och utbildare och göra det lättare att förvärva cyberkompetens, bland annat genom lärlingsutbildningar. De bör uppmuntra åtgärder för att integrera cybersäkerhet i utbildningsprogram, och samtidigt säkerställa deras tillgänglighet, utveckla utbudet av **lärlingsutbildningar** och praktikplatser, främja innovativa strategier, till exempel seriösa spel och gemensamma simuleringsplattformar, anordna prova-på-veckor i cybersäkerhetstjänster och förklara de icke-tekniska yrkesprofilerna. De bör även underlätta för grupper som är svåra att nå, såsom ungdomar med funktionsnedsättning, som bor i avlägsna områden eller landsbygdsområden och ungdomar som tillhör andra minoritetsgrupper, att delta i dessa cybersäkerhetsutbildningar.

Kommissionen kommer även i fortsättningen att stödja utvecklingen av mikromeriter och yrkesutbildningsprogram. Till exempel kommer **gemensamma kandidat- och masterexamina, gemensamma kurser eller moduler som kan leda till mikromeriter** och

[58] Se det gemensamma meddelandet till Europaparlamentet och rådet, *EU:s politik för cyberförsvar*, JOIN(2022) 49 final.

[59] Här kommer uppmärksamhet att ägnas åt arbetet med den kompetensram för utbildning om it-brottslighet som för närvarande håller på att utarbetas.

[60] Till exempel den europeiska klassificeringen av färdigheter, kvalifikationer och yrken (Esco), Europass, det europeiska nätverket för arbetsförmedlingar (Eures).

[61] I CyberSecPro kommer man till exempel att genomföra en analys av de program, kurser och sommarskolor inom cybersäkerhet som universiteten erbjuder och av de betygstabeller som används inom det europeiska systemet för överföring och ackumulering av studiemeriter (ECTS). Man kommer också att säkerställa att antalet praktikanter under treårsperioden minst uppgår till det fastställda målet på 530 praktikanter och utbilda externa personer från olika branscher och sektorer.

blandade intensivprogram[62] i alla ämnen, inbegripet **cybersäkerhet**, att fortsätta att finansieras inom ramen för Erasmus+. Det fortsatta genomförandet av **initiativet Europauniversitet**[63] och **yrkeskunskapscentrum**[64] kommer också att stödjas för att uppmuntra till ökat samarbete mellan högre utbildningsanstalter och relevanta yrkesutbildningsanstalter i hela Europa. Detta mål om ett fördjupat samarbete kommer att stödjas inom ramen för EU:s finansieringsprogram, däribland Erasmus+ och programmet för ett digitalt Europa, liksom med EU-medel för utveckling av **individuella utbildningskonton**[65].

För att göra det lättare för den akademiska världen och anordnare av cybersäkerhetsutbildning på nationell nivå att samarbeta med arbetsgivare inom den privata och den offentliga sektorn och främja synergier mellan den offentliga och den privata sektorn uppmanas de nationella samordningscentrumen att undersöka möjligheterna att inrätta **cybercampus** i medlemsstaterna. Syftet med cybercampus skulle vara att fungera som kompetenscentrum på nationell nivå för cybersäkerhetsgemenskapen, och akademin skulle underlätta deras nätverksbyggande och främja samordning av deras verksamheter.

Enisa kommer att förbättra sitt utbud av cybersäkerhetsutbildningar genom att anpassa **sin kurskatalog**[66] till den europeiska kompetensramens profiler och utarbeta utbildningsmoduler för olika profiler, vilket kan förbättra medlemsstaternas utbildningsutbud. Enisa kommer också att utöka sitt **instruktörsutbildningsprogram**[67] för att tillgodose de yrkesmässiga behov som EU:s institutioner, organ och byråer samt medlemsstaternas offentliga myndigheter och **offentliga och privata kritiska operatörer** har inom ramen för NIS 2-direktivet.

Dessutom kommer andra EU-byråer och EU-organ att stärka sitt utbud av cybersäkerhetsutbildningar. Vid genomförandet av EU:s politik för cyberförsvar kommer **Esfa** till exempel att utveckla en ny uppsättning cybersäkerhetskurser och anpassa vissa av sina nuvarande kurser till den europeiska kompetensramen. Dessa kurser kommer att leda till certifiering av läranderesultaten[68]. Esfa kommer i samarbete med kommissionen att undersöka möjligheten att integrera certifikat i EUeID-plånboken. Esfa kommer även att undersöka möjliga kompetensbedömningsmekanismer, som kommer att användas vid utfärdande av certifikat. När det gäller bekämpandet av cyberbrottslighet kommer man också att verka för nära band till Cepols akademi mot cyberbrottslighet[69], för att främja synergier och komplementaritet i utformningen och genomförandet av läroplaner.

4.3. Skapa synergier och synliggöra cybersäkerhetsutbildningar och cybersäkerhetscertifiering i medlemsstaterna

[62] Vid blandade intensivprogram kombineras undervisning på nätet med en kort period av fysisk mobilitet.

[63] Initiativet Europauniversitet | Det europeiska området för utbildning (europa.eu).

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

[65] I enlighet med rådets rekommendation av den 16 juni 2022 om individuella utbildningskonton.

[66] Utbildningskurser – Enisa (europa.eu).

[67] Instruktörsutbildningsprogram – Enisa (europa.eu).

[68] I enlighet med artikel 20.4 i rådets beslut (Gusp) 2020/1515 av den 19 oktober 2020 om inrättande av en europeisk säkerhets- och försvarsakademi och om upphävande av beslut (Gusp) 2016/2382.

[69] Cepols akademi mot cyberbrottslighet inrättades 2019 för att tillhandahålla en förstklassig plattform för att förbättra kunskaperna om cyberbrottslighet och cyberkapaciteten i Europa.

Akademin bör ta upp frågan om synlighet och synergier när det gäller utbildning och certifiering. Detta skulle gynna de civila, försvarsrelaterade, brottsbekämpande och diplomatiska cybergemenskaperna, eftersom alla sektorer i många fall behöver samma sakkunskap, baserad på liknande läroplaner och läranderesultat.

Akademin skulle tillhandahålla en **gemensam kontaktpunkt** för dem som är intresserade av en cybersäkerhetskarriär. På kort sikt kommer detta att göras genom att stärka **kommissionens plattform för digital kompetens och digitala arbetstillfällen** med stöd av ECCO-projektet. En särskild sektion om cybersäkerhetskarriärer kommer att kopplas ihop med befintliga verktyg, från högre utbildningsprogram till andra lärandemöjligheter, inklusive kurser som leder till mikromeriter och yrkesutbildningsprogram som leder till jobberbjudanden. Man kommer att uppnå detta genom att hänvisa till eller integrera pågående insatser och initiativ i plattformen, till exempel Enisas, som i samarbete med den akademiska världen har gjort en **kartläggning av utbildningsinstitutioner** som tillhandahåller cybersäkerhetsprogram. Detta kommer att förbättras ytterligare med stöd av de nationella samordningscentrumen. Dessutom kommer två **register över befintliga utbildningar från den offentliga och den privata sektorn och cybersäkerhetscertifieringar** att utvecklas och konsolideras av Enisa med stöd av nationella samordningscentrum, kommissionen och ECCO-projektet, och i samarbete med enheter som utfärdar certifieringar och även bygger vidare på andra relevanta initiativ[70]. Dessa kommer också att integreras i den gemensamma kontaktpunkten för plattformen för digital kompetens och digitala arbetstillfällen. Detta arbete kommer också att gynna de nationella samordningscentrumen, vars uppgift särskilt är att främja och sprida utbildningsprogram om cybersäkerhet[71].

Det är också nödvändigt att ge yrkesutövarna garantier för att den utbildning de genomför är av erforderlig kvalitet. Här kommer Enisa att utveckla ett **pilotprojekt** för att undersöka möjligheterna att inrätta ett europeiskt certifieringssystem för cybersäkerhetskompetens.

Dessutom är det mycket viktigt att identifiera färdigheter och utbildningar och koppla dem till en yrkesprofil. Det är dock också viktigt att säkerställa att cybersäkerhetstjänsterna förses med den kompetens, sakkunskap och erfarenhet som krävs. Detta gäller särskilt leverantörer av förvaltade säkerhetstjänster på områden som incidenthantering, penetrationstester, säkerhetsrevisioner och konsulttjänster. I NIS 2-direktivet och förslaget till cybersolidaritetsakt fastställs särskilda uppgifter för sådana leverantörer av förvaltade säkerhetstjänster. Därför föreslår kommissionen också en **riktad ändring av cybersäkerhetsförordningen**[72] för att möjliggöra certifieringssystem för förvaltade säkerhetstjänster på EU-nivå. Sådana certifieringssystem bör bland annat syfta till att säkerställa att dessa tjänster tillhandahålls av personal med mycket hög teknisk kunskap och kompetens på de relevanta områdena.

Mekanismer för kvalitetssäkring och erkännande av mikromeriter[73] bidrar till att göra läranderesultaten tydliga, jämförbara och överförbara. I enlighet med rådets rekommendation

[70] Till exempel W4C-akademin – Women4Cyber eller projektet för global certifiering av it-brottslighet för brottsbekämpande och rättsliga myndigheter.

[71] ”1. De nationella samordningscentrumen ska ha följande uppgifter: (...) g) Utan att det påverkar medlemsstaternas befogenheter på utbildningsområdet och med beaktande av Enisas relevanta uppgifter, samarbeta med nationella myndigheter om eventuella bidrag till att främja och sprida utbildningsprogram om cybersäkerhet”, artikel 7.1 g i ECCC-förordningen. Se även skäl 28.

[72] Europaparlamentets och rådets förordning (EU) 2019/881 av den 17 april 2019 om Enisa (Europeiska unionens cybersäkerhetsbyrå) och om cybersäkerhetscertifiering av informations- och kommunikationsteknik och om upphävande av förordning (EU) nr 526/2013 (cybersäkerhetsakten).

[73] Till exempel dokumentation eller intyg om läranderesultat som människor förvärvar efter kortare utbildningar.

om en europeisk strategi för mikromeriter[74] uppmanas medlemsstaterna att inkludera mikromeriter för cybersäkerhet i sina nationella referensramar för kvalifikationer. På så sätt skulle de kunna koppla mikromeriterna för cybersäkerhet till den europeiska referensramen för kvalifikationer[75]. Det finns en infrastruktur för europeiska digitala lärandeintyg för att utfärda digitalt signerade cybersäkerhetskvalifikationer och mikromeriter för enskilda personer. Dessa är rika på data om bland annat läranderesultat inom cybersäkerhet, och kan lagras i den framtida **digitala plånboken EUeID**[76].

Åtgärder inom akademin

Medlemsstaterna och näringslivet

- Säkerställa stöd för utveckling och erkännande av **mikromeriter** för lärande inom cybersäkerhet, i enlighet med rådets rekommendation om en europeisk strategi för mikromeriter.
- Inkludera cybersäkerhetskvalifikationer, inklusive mikromeriter i de **nationella referensramarna för kvalifikationer**.
- Ge **möjlighet till arbetsplatsanknuten utbildning** genom lärlingsutbildningar för personer som genomgår initiativ för kompetensutveckling inom cybersäkerhet.

Kommissionen

- På kort sikt skapa **en gemensam kontaktpunkt** för cybersäkerhetsprogram, befintliga utbildningar och cybersäkerhetscertifiering via **plattformen för digital kompetens och digitala arbetstillfällen** senast i slutet av 2023.
- Lägga fram ett förslag till ändring av **förordningen om cybersäkerhet** för att möjliggöra certifiering av leverantörer av förvaltade säkerhetstjänster den 18 april 2023.

EU:s organ och byråer

- Inrätta den **europeiska kompetensramen för cybersäkerhet** som en gemensam strategi för yrkesprofiler inom cybersäkerhet och tillhörande färdigheter senast i slutet av 2023.
- Enisa ska börja utveckla ett pilotprojekt om att införa ett **europeiskt certifieringssystem** för cybersäkerhetskompetens under andra kvartalet 2023.
- Enisa ska se över sin **kurskatalog** och inleda sitt **instruktörsutbildningsprogram** för offentliga och privata kritiska operatörer senast i slutet av 2023.
- Slutföra **anpassningen av Esfas kursplaner till den europeiska kompetensramen för cybersäkerhet** senast i mitten av 2023.

5. Berörda parters deltagande: åtaganden för att minska kompetensbristen inom cybersäkerhet

Inom ramen för akademin kommer en samordnad strategi för berörda parters deltagande att utvecklas för att komma till rätta med kompetensbristen inom cybersäkerhet. Syftet kommer

[74] Rådets rekommendation om en europeisk strategi för mikromeriter för livslångt lärande och anställbarhet.

[75] Rådets rekommendation av den 22 maj 2017 om den europeiska referensramen för kvalifikationer för livslångt lärande och om upphävande av Europaparlamentets och rådets rekommendation av den 23 april 2008 om en europeisk referensram för kvalifikationer för livslångt lärande.

[76] Förslag till Europaparlamentets och rådets förordning om ändring av förordning (EU) nr 910/2014 vad gäller inrättandet av en ram för europeisk digital identitet.

att vara att maximera synligheten och effekterna av de olika aktörernas åtaganden för att minska kompetensbristen inom cybersäkerhet.

Kommissionen uppmanar berörda parter att göra konkreta åtaganden i form av utfästelser om att kompetensutveckla och omskola arbetstagarna genom riktade åtgärder, som i största möjliga utsträckning bygger på den identifierade kompetensbristen inom cybersäkerhet. **Aktörernas utfästelser om cybersäkerhet** bör rapporteras på **plattformen för digital kompetens och digitala arbetstillfällen**, i likhet med andra digitala utfästelser som redan visas på plattformen. Kommissionen uppmuntrar vidare de berörda parter som gör ett cybersäkerhetsåtagande på plattformen att ansluta sig till det **digitala storskaliga partnerskapet inom pakten för kompetens**[77]. Den ser gärna att de cybersäkerhetsåtaganden som görs inom ramen för det digitala storskaliga partnerskapet läggs upp på plattformen för digital kompetens och digitala arbetstillfällen. På samma sätt ser den gärna att de åtaganden som görs inom ramen för plattformen för digital kompetens och digitala arbetstillfällen rapporteras inom ramen för kompetenspaktens digitala storskaliga partnerskap.

Kommissionen uppmanar vidare medlemsstaterna att **fortsätta sina ansträngningar för att genomföra förklaringen Women in Digital**[78] för att uppmuntra kvinnor att spela en aktiv och framträdande roll inom den digitala tekniksektorn och uppnå en jämnare könsfördelning i cybersäkerhetsyrken. Kommissionen uppmuntrar också medlemsstaterna att utveckla synergier med sina program inom **Europeiska socialfonden+** (ESF+) för att ytterligare stödja jämställdhetsmålet när det gäller deltagande på arbetsmarknaden[79], till exempel genom att inrätta **mentorprogram för flickor och kvinnor**. Dessa kan underlätta skapandet av förebilder för att locka flickor till cybersäkerhetsyrken och samtidigt bekämpa könsstereotyper. Det främjar också kvinnors kompetensutveckling och omskolning och hjälper till att utveckla en gemenskap som kan hjälpa kvinnor att komma in på eller befordras på arbetsmarknaden inom cybersäkerhet.

Medlemsstaterna bör, som en del av **sina nationella cybersäkerhetsstrategier, anta särskilda åtgärder i syfte att minska kompetensbristen inom cybersäkerhet**[80], identifiera och bättre kanalisera insatser för att minska kompetensbristen och i slutändan säkerställa ett korrekt genomförande av sina skyldigheter enligt NIS 2-direktivet.

Vissa medlemsstater utnyttjar **synergier mellan civila initiativ, försvarsinitiativ och initiativ för brottsbekämpning**. Genom att till exempel utveckla arbetsstyrkan med hjälp av den nationella värnplikten, eller använda sig av cyberreservare, som är militärt utbildade medborgare som innehar cybersäkerhetstjänster inom försvarsmakten[81], kan befolkningen, särskilt unga vuxna, öka sin kompetens inom cybersäkerhet och cyberförsvar. Detsamma gäller **kampen mot it-brottslighet**, eftersom det finns många likheter mellan de allmänna cybersäkerhetsinsatserna och de brottsbekämpande åtgärderna vid hantering av cyberincidenter. Kommissionen uppmuntrar medlemsstaterna att diskutera sådana initiativ

[77] Nya europeiska partnerskap för att förverkliga EU:s ambitioner för det digitala decenniet | Att forma EU:s digitala framtid (europa.eu), bildades inom ramen för pakten för kompetens för att komma till rätta med bristen på informations- och kommunikationsteknik (IKT).

[78] EU-länder åtar sig att öka kvinnors deltagande i den digitala sektorn | Att forma EU:s digitala framtid (europa.eu).

[79] Europaparlamentets och rådets förordning (EU) 2021/1057 av den 24 juni 2021 om inrättande av Europeiska socialfonden+ (ESF+) och om upphävande av förordning (EU) nr 1296/2013, artikel 4.1 c.

[80] NIS 2-direktivet, artikel 7.2 f.

[81] Rapport – *Cyber Conscription: Experience and Best Practice from Selected Countries*, *Martin Hurt och Tiia Sõmer*, *International Centre for Defence and Security*, februari 2021.

med varandra och uppmanar dem att bedöma hur en kvalificerad arbetsstyrka bäst kan verka inom både de försvarsrelaterade och civila cybersäkerhetsgemenskaperna.

Kommissionen kommer att överväga förslag på hur man kan komma till rätta med rådande och förväntade brister som den identifierat vid sin granskning av behoven vid EU:s institutioner, organ och byråer. Den kommer särskilt att uppmuntra personalen att utnyttja **EU:s och Förenta staternas** kommande **cybersäkerhetsstipendium** som inrättats inom ramen för dialogen mellan EU och Förenta staterna.

Åtgärder inom akademin

Näringslivet

- Föreslå specifika **utfästelser om cybersäkerhet** på plattformen för digital kompetens och digitala arbetstillfällen den 18 april 2023.

Medlemsstaterna

- I de **nationella cybersäkerhetsstrategierna** inkludera särskilda åtgärder för att minska kompetensbristen inom cybersäkerhet.

Medlemsstaterna och näringslivet

- Genomföra förklaringen Women in Digital och uppnå en **jämnare könsfördelning i cybersäkerhetsyrken** senast 2030.

6. Finansiering: skapa synergier för att maximera effekterna av satsningar på kompetensutveckling inom cybersäkerhet

Inom ramen för akademin kommer man att maximera effekterna av investeringar i cybersäkerhetskompetens genom att tillhandahålla en gemensam kontaktpunkt, möjliggöra en bättre kanalisering av medel för att tillgodose marknadens behov och integrera användningen av finansiering, för att möjliggöra synergier mellan olika instrument och samtidigt undvika dubbelarbete[82].

6.1. Matcha medel med behov

Inom ramen för akademin kommer ECCC, med stöd av kommissionen, ECCO-projektet och de nationella samordningscentrumen, att samla in **information om hur EU-medel används för att finansiera cybersäkerhetskompetens** och bedöma hur EU-medel hjälper till att minska kompetensbristen inom cybersäkerhet. Med beaktande av denna aggregerade information kommer ECCC att sträva efter en bättre kanalisering av EU-medel för att tillgodose de identifierade behoven. ECCC kommer att finansiera åtgärder för att komma till rätta med de mest akuta bristerna på arbetskraft på cybersäkerhetsområdet, inbegripet de som rör genomförandet av cybersäkerhetspolitiska behov.

6.2. Synliggöra tillgängliga medel och partnerskapsinitiativ för cybersäkerhetskompetens

[82] Finansieringsmöjligheter (europa.eu) Stödtjänsterna inom pakten för kompetens utgör en gemensam kontaktpunkt för information om kompetensfinansiering, bland annat för det digitala ekosystemet. Inom ramen för paktens stödtjänster tillhandahålls allmän information om finansieringsinstrument som inte är specifikt inriktade på cybersäkerhetskompetens, men akademin bör ta hänsyn till deras arbete för att undvika dubbelarbete.

På kort sikt kommer **plattformen för digital kompetens och digitala arbetstillfällen** att bli en gemensam kontaktpunkt för berörda parter, där all information om finansieringsmöjligheter för cybersäkerhetskompetens kommer att finnas tillgänglig.

EU investerar i människor och deras kompetens och använder partnerskap, t.ex. med näringslivet, för att mobilisera insatser för kompetensutveckling och omskolning inom ramen för flera instrument som fastställs i den **europeiska kompetensagendan**[83], särskilt **pakten för kompetens**[84] och **handlingsplanen för digital utbildning**[85]. Programmet för ett digitalt Europa finansierar kompetensmöjligheter inom cybersäkerhet, särskilt genom projektinitiativ som omfattar flera länder vilket tydligt kompletterar det stöd som Horisont Europa erbjuder för forskning och innovativa tekniska lösningar på cybersäkerhetsområdet. **Europeiska försvarsfonden**[86] finansierar forskning och teknisk utveckling för att genomföra effektiva cyberinsatser, inbegripet utbildning och övningar[87]. **Erasmus+** kommer att fortsätta att stödja sådana initiativ, bland annat genom blandade intensivprogram och samarbetsprojekt.

Medlemsstaterna uppmanas att mobilisera de EU-medel som de direkt förvaltar för att stödja kompetens och arbetstillfällen inom cybersäkerhet. De sammanhållningspolitiska fonderna, t.ex. **Europeiska regionala utvecklingsfonden (Eruf)** och **ESF+**, innebär stora möjligheter för synergier[88]. **Faciliteten för återhämtning och resiliens**[89] och **InvestEU**[90] omfattar ytterligare viktiga komplementära åtgärder för att nå akademins mål.

Åtgärder inom akademin

Europeiska kompetenscentrumet för cybersäkerhet och Enisa

- **Kartlägga** befintlig EU-finansiering för cybersäkerhetskompetens i förhållande till marknadens behov, bedöma **ändamålsenligheten** och fastställa **finansieringsprioriteringar** senast i slutet av 2024.

Kommissionen

- Skapa en **gemensam kontaktpunkt** för finansieringsmöjligheter för cybersäkerhetskompetens på plattformen för digital kompetens och digitala arbetstillfällen senast i slutet av 2023.

[83] Den europeiska kompetensagendan – Sysselsättning, socialpolitik och inkludering – Europeiska kommissionen (europa.eu).

[84] EU:s finansieringsinstrument för kompetensutveckling och omskolning – Sysselsättning, socialpolitik och inkludering – Europeiska kommissionen (europa.eu).

[85] Handlingsplanen för digital utbildning 2021–2027.

[86] Europaparlamentets och rådets förordning (EU) 2021/697 av den 29 april 2021 om inrättande av Europeiska försvarsfonden och om upphävande av förordning (EU) 2018/1092.

[87] Medlemsstaterna har åtagit sig att delta i gemensamma utbildningar och övningar, till exempel genom att inrätta och delta i cyberutbildnings- och cyberövningsprojekt inom ramen för permanent strukturerat samarbete (Pesco), såsom EU:s cyberakademi och innovationsknutpunkt (EU CAIH) och Federated Cyber Ranges.

[88] Artikel 3.1 i förordning (EU) 2021/1058 och artikel 4.1 g i förordning (EU) 2021/1057.

[89] Till exempel planerar Estland i sin återhämtnings- och resiliensplan att investera (10 miljoner euro) i digitala färdigheter, och kommer bland annat att se över utbildningarna för IKT-experter, finansiera kompetensutveckling och omskolning av IKT-specialister inom cybersäkerhet och bidra till utvecklingen av ett pilotprogram för att omforma kvalifikationsramen för IKT-specialister.

[90] Berörda parter (t.ex. utbildningsleverantörer och företag som vill utforma eller förbättra sin cybersäkerhetsutbildning) kan kontakta InvestEU:s rådgivningscentrum, som erbjuder projektutvecklare och företag tekniskt stöd och bistånd, bland annat för kapacitetsuppbyggnad, och kan söka information på InvestEU-portalen.

7. Mäta framstegen: inbyggd ansvarsskyldighet

Inom ramen för akademin kommer **metoder** att utvecklas som gör det möjligt att **mäta de framsteg som görs för att minska kompetensbristen inom cybersäkerhet**.

7.1. Fastställande av cybersäkerhetsindikatorer för att följa utvecklingen på arbetsmarknaden för cybersäkerhet

Indexet för digital ekonomi och digitalt samhälle (Desi) sammanfattar indikatorer om Europas digitala resultat och följer medlemsstaternas framsteg. Inom ramen för akademin för cyberkompetens kommer Enisa, i samarbete med kommissionen och samarbetsgruppen för nät- och informationssäkerhet[91], att ta fram **indikatorer**, bland annat när det gäller kön, för att följa de framsteg som görs i medlemsstaterna för att öka antalet yrkesverksamma inom cybersäkerhet, i samråd med berörda marknadsaktörer och de nationella samordningscentrumen. Enisa kommer att använda Desis metoder[92] och se till att indikatorerna ligger i linje med Europas digitala mål för IKT-personal och för att uppnå en jämnare könsfördelning inom IKT. Kommissionen kommer sedan att arbeta för att integrera sådana indikatorer i Desi, vilket gör det möjligt att årligen följa upp läget på cyberkompetensområdet och arbetsmarknaden.

7.2. Insamling av uppgifter och rapportering

Enisa kommer att samla in uppgifter om indikatorerna med stöd av ECCO-projektet och de nationella samordningscentrumen. På grundval av de insamlade uppgifterna kommer Enisa att utarbeta en **årlig rapport** som kommer att bidra till lägesrapporten om det digitala decenniet[93], som tillsammans med Desi kommer att bidra ytterligare till den **europeiska planeringsterminens** landspecifika analyser och rekommendationer[94]. Dessutom kommer indikatorerna för cybersäkerhetskompetens att bidra till den **rapport som Enisa antar vartannat år** om cybersäkerhetssituationen i EU i enlighet med NIS 2-direktivet, som omfattar cybersäkerhetskapacitet, cybersäkerhetsmedvetenhet och cyberhygien i hela EU.

7.3. Utarbetande av centrala resultatindikatorer för cybersäkerhet

I syfte att minska den europeiska kompetensbristen inom cybersäkerhet kommer Enisa, i nära samarbete med kommissionen och de nationella samordningscentrumen, att föreslå centrala resultatindikatorer för kommissionen, med utgångspunkt i metoderna från policyprogrammet för det digitala decenniet 2030 samt näringslivets erfarenheter. Enisa kommer att ta vederbörlig hänsyn till de centrala resultatindikatorer som medlemsstaterna använder för att bedöma sina nationella cybersäkerhetsstrategier[95].

Åtgärder inom akademin

Enisa

[91] Använda och komplettera de metoder som Enisa ska utarbeta i den rapport om cybersäkerhetssituationen i unionen som byrån antar vartannat år i enlighet med artikel 18.3 i NIS 2-direktivet.

[92] Se metodbeskrivningen *Methodological note* för indexet för digital ekonomi och digitalt samhälle (Desi) 2022 på Indexet för digital ekonomi och digitalt samhälle (Desi) | Att forma EU:s digitala framtid (europa.eu).

[93] Europaparlamentets och rådets beslut (EU) 2022/2481 av den 14 december 2022 om inrättande av policyprogrammet för det digitala decenniet 2030.

[94] Ibid, skäl 25.

[95] NIS 2-direktivet, artikel 7.4.

- Utarbeta **indikatorer och centrala resultatindikatorer** för cybersäkerhetskompetens senast i slutet av 2023.
- **Samla in uppgifter** om indikatorer och rapportera om dem, med en första insamling senast 2025.

Kommissionen

- Arbeta för att integrera **cybersäkerhetsindikatorer i Desi** och i **lägesrapporten om det digitala decenniet**.

8. Slutsats

Detta meddelande lägger grunden för en omarbetning av EU:s strategi för att öka cybersäkerhetskompetensen för yrkesverksamma i EU. Syftet är att minska den kompetensbrist som råder på cybersäkerhetsområdet och utrusta EU med den arbetskraft som krävs för att kunna hantera den ständigt föränderliga hotbilden, genomföra EU-politik som syftar till att skydda EU från cyberattacker, men också främja affärsmöjligheter och konkurrenskraft. En kvalificerad arbetsstyrka inom cybersäkerhet kan gynna de **civila, försvarsrelaterade, diplomatiska och brottsbekämpande** gemenskaperna och underlätta synergier dem emellan.

Kommissionen uppmanar medlemsländerna och alla berörda parter att förverkliga ambitionen med akademin för cyberkompetens.