EUROPESE
COMMISSIE

Straatsburg, 18.4.2023
COM(2023) 207 final

MEDEDELING VAN DE COMMISSIE AAN HET EUROPEES PARLEMENT EN DE RAAD

Wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de veerkracht van Europa te versterken (“De academie voor cyberbeveiligingsvaardigheden”)

Wegwerken van het tekort aan cyberbeveiligingsprofessionals om het concurrentievermogen, de groei en de veerkracht van Europa te versterken ("De academie voor cyberbeveiligingsvaardigheden")

1. Dringende noodzaak om risico's te beperken door het tekort aan en de lacunes op het gebied van cyberbeveiligingsvaardigheden aan te pakken

Cyberbeveiliging maakt niet alleen deel uit van de beveiliging van burgers, bedrijven en lidstaten, maar is ook noodzakelijk om de politieke stabiliteit van de EU, de stabiliteit van haar democratieën en de welvaart van onze samenleving en bedrijven te waarborgen. Het **dreigingslandschap** op het gebied van cyberbeveiliging is de afgelopen jaren sterk geëvolueerd en er is de zorgwekkende trend dat steeds meer cyberaanvallen gericht zijn tegen kritieke militaire en civiele infrastructuur in de EU. Dreigingsactoren vergroten hun capaciteiten en er ontstaan nieuwe, hybride en opkomende dreigingen, zoals het gebruik van bots en technieken op basis van artificiële intelligentie[1]. Vooral dreigingen met gijzelsoftware ("ransomware") brengen entiteiten stelselmatig aanzienlijke financiële en reputatieschade toe[2].

Een groot aantal cyberbeveiligingsincidenten trof bovendien overheidsdiensten en regeringen in de lidstaten, alsmede instellingen, organen en instanties van de Unie[3]. Ook de financiële sector[4] en de zorgsector[5], beide essentiële pijlers van onze samenleving en economie, zijn keer op keer doelwit geweest[6]. De geopolitieke spanningen vanwege de Russische aanvalsoorlog tegen Oekraïne hebben de dreiging op het gebied van cyberbeveiliging vergroot[7] en kunnen onze samenleving destabiliseren. De **veiligheid** van de EU kan niet worden gegarandeerd zonder de **meest waardevolle troef van de EU: haar bevolking.** De EU heeft dringend behoefte aan professionals met vaardigheden en competenties om cyberaanvallen te voorkomen, op te sporen en tegen te gaan, de EU en haar meest kritieke infrastructuur daartegen te beschermen en haar **veerkracht** te waarborgen.

Het tekort aan cyberbeveiligingsprofessionals belemmert voorts het **concurrentievermogen** en de **groei** van Europa, die sterk afhankelijk zijn van de ontwikkeling en toepassing van strategische digitale technologieën (bv. artificiële intelligentie, 5G en cloud). Er zijn

---

[1] ENISA Threat Landscape 2022 – Enisa (europa.eu).

[2] Internet Organised Crime Threat Assessment (Iocta) 2021, Europol. Actoren die met gijzelsoftware dreigen, bouwen voort op het model "Ransomware-as-a-Service". De jaarlijkse kosten voor bedrijven bedroegen in 2022 meer dan 18,4 miljard EUR (verslag 2022 van Cybereason over de ware kosten van gijzelsoftware).

[3] Zie bijvoorbeeld de gezamenlijke publicatie van Enisa en CERT-EU, JP-23-01 – Sustained activity by specific threat actors, TLP:CLEAR, 15 februari 2023.

[4] In Duitsland was bijvoorbeeld 90 % van de tussen 1 juni 2021 en 31 mei 2022 gemelde fraude in het mailverkeer financiële phishing. Ook vond er een aanval plaats op een bedrijf in de financiële sector waarbij meer dan 20 000 besmette apparaten uit 125 landen werden ingezet (The State of IT Security in Germany in 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI), 1 januari 2023).

[5] In Frankrijk zijn bijvoorbeeld gijzelsoftwareaanvallen uitgevoerd op openbare zorginstellingen, zoals het Centre Hospitalier Sud Francilien, waarbij 11 GB aan persoonlijke en medische gegevens alsook personeelsgerelateerde gegevens werden gecompromitteerd en gepubliceerd door de dreigingsactor (Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), januari 2023).

[6] ENISA Threat Landscape 2022.

[7] Zie ook: CERT-EU – Russia's war on Ukraine: one year of cyber operations (europa.eu); Russische cyberoperaties tegen Oekraïne: verklaring van de hoge vertegenwoordiger namens de EU, 10 mei 2022; verklaring van de hoge vertegenwoordiger namens de Europese Unie over kwaadwillige cyberactiviteiten van hackers en hackergroepen in de context van de Russische agressie tegen Oekraïne, 19 juli 2022.

geschoolde arbeidskrachten op het gebied van cyberbeveiliging nodig om ervoor te zorgen dat de EU in staat blijft om in een mondiale context belangrijke geavanceerde technologieën te leveren.

De EU heeft de afgelopen jaren aanzienlijke vooruitgang geboekt met haar cyberbeveiligingsbeleid om zich voor te bereiden op en het hoofd te bieden aan dit evoluerende dreigingslandschap. In dit verband zijn diverse initiatieven vastgesteld, zoals de EU-strategie inzake cyberbeveiliging voor het digitale tijdperk[8], de herziene richtlijn beveiliging van netwerk- en informatiesystemen (NIS2-richtlijn)[9], de sectorale EU-cyberbeveiligingswetgeving[10], het EU-beleid op het gebied van cyberdefensie[11], de verordening cyberweerbaarheid[12] en de door de Commissie samen met deze mededeling voorgestelde verordening cybersolidariteit. Zonder de nodige geschoolde arbeidskrachten om deze initiatieven uit te voeren, zullen de doelstellingen van deze wetgeving echter niet worden verwezenlijkt. De basiskennis van de algemene bevolking op het vlak van cyberbeveiliging wordt weliswaar aangepakt in initiatieven ter ondersteuning van de ontwikkeling van algemene vaardigheden die nodig zijn om aan de samenleving deel te nemen[13], maar een competente beroepsbevolking in zowel de publieke als de particuliere sector en op zowel nationaal als EU-niveau, onder meer in normalisatie-instellingen, is van essentieel belang om **aan die wettelijke en beleidseisen op het gebied van cyberbeveiliging te voldoen**.

De veiligheid en het concurrentievermogen van de EU zijn dus afhankelijk van professioneel cyberbeveiligingspersoneel. De EU kampt echter met een zeer groot tekort aan geschoolde cyberbeveiligingsprofessionals, waardoor de EU en haar lidstaten, bedrijven en burgers blootstaan aan het risico op cyberbeveiligingsincidenten. In 2022 was er een tekort van **260 000**[14] **tot 500 000**[15] cyberbeveiligingsprofessionals in de EU en werd het aantal vereiste cyberbeveiligingsprofessionals geraamd op 883 000[16], hetgeen duidt op een discrepantie tussen de beschikbare en de door de arbeidsmarkt gevraagde competenties. De cyberbeveiligingssector heeft tevens te lijden onder misvattingen in verband met het

[8] Gezamenlijke mededeling aan het Europees Parlement en de Raad, De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk, JOIN(2020) 18 final.

[9] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

[10] Voor de financiële sector bijvoorbeeld Verordening (EU) 2022/2554 van het Europees Parlement en de Raad van 14 december 2022 betreffende digitale operationele weerbaarheid voor de financiële sector en tot wijziging van Verordeningen (EG) nr. 1060/2009, (EU) nr. 648/2012, (EU) nr. 600/2014, (EU) nr. 909/2014 en (EU) 2016/1011 (DORA).

[11] Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

[12] Voorstel voor een verordening van het Europees Parlement en de Raad betreffende horizontale cyberbeveiligingsvereisten voor producten met digitale elementen en tot wijziging van Verordening (EU) 2019/1020, COM(2022) 454 final.

[13] Tot de relevante initiatieven op het vlak van algemene digitale vaardigheden voor de bevolking behoren: de doelstelling van het actieplan voor de Europese pijler van sociale rechten en het digitale kompas om ervoor te zorgen dat 80 % van de bevolking tegen 2030 over digitale basisvaardigheden beschikt, het actieplan voor digitaal onderwijs 2021-2027, het kaderinstrument inzake digitale competentie en het voorstel voor een aanbeveling van de Raad over de verbetering van het aanbod van digitale vaardigheden in onderwijs en opleiding.

[14] (ISC)² in Assessing Cyber Skills on the basis of the ECSF, Enisa-webinar, 16 februari 2023.

[15] Volgens de Europese organisatie voor cyberbeveiliging (ECSO), zoals uiteengezet in de Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

[16] (ISC²) in Assessing Cyber Skills on the basis of the ECSF, Enisa-webinar, 16 februari 2023.

technische imago van cyberbeveiliging en blijft weinig aantrekkelijk voor **vrouwen**, die 20 % van de afgestudeerden in cyberbeveiliging[17] en 19 % van de specialisten in informatie- en communicatietechnologie (ICT)[18] uitmaken. Om hier iets aan te doen, is in het **beleidsprogramma voor het digitale decennium tot 2030**[19] het doel vastgesteld om het aantal ICT-professionals uiterlijk in 2030 tot 20 miljoen te verhogen en tegelijkertijd een genderevenwicht te bereiken. Bovendien vereist de uitvoering van nieuw EU-beleid goed geschoolde en voldoende arbeidskrachten; zo wees meer dan 42 % van de hogere IT-leidinggevenden in de financiëledienstensector het gebrek aan cyberbeveiligingsvaardigheden en -expertise aan als een belangrijke uitdaging voor hun bedrijf met betrekking tot cyberbeveiliging en incidentenbeheer[20], en dat op een moment dat zij sectorale cyberbeveiligingswetgeving, zoals de verordening digitale operationele weerbaarheid (DORA), moeten uitvoeren.

Het feit dat werkgevers terughoudend zijn om in menselijk kapitaal te investeren en op zoek gaan naar reeds opgeleide en ervaren arbeidskrachten, draagt verder bij tot een inperking van de arbeidsmarkt[21]. Dit tekort treft alle soorten ondernemingen, met inbegrip van kleine en middelgrote ondernemingen (**kmo's**), die 99 % van alle bedrijven in de EU uitmaken[22]. Ook **overheidsinstanties**, die in hoge mate worden getroffen door cyberbeveiligingsincidenten en daar de meeste gevolgen van ondervinden, staan voor een grote uitdaging[23].

Het tekort aan cyberbeveiligingsprofessionals in de EU moet dan ook dringend worden weggewerkt, aangezien de veiligheid en het concurrentievermogen van de EU op het spel staan.

2. Gebrek aan synergieën en gecoördineerde maatregelen om de lacunes op het gebied van cyberbeveiligingsvaardigheden op te vullen

Er zijn steeds meer Europese en nationale initiatieven van publieke en private entiteiten om de tekorten op de arbeidsmarkt voor cyberbeveiliging aan te pakken. Deze initiatieven zijn echter versnipperd en hebben tot nu toe niet de kritische massa bereikt die nodig is om echt een verschil te maken.

Om te beginnen is er momenteel slechts beperkte overeenstemming over de functieprofielen en bijbehorende vaardigheden voor cyberbeveiligingsarbeidskrachten, terwijl voor vergelijkbare cyberbeveiligingsfuncties dezelfde vaardigheden vereist zouden moeten zijn. De geringe populariteit van een **Europees referentiekader voor cyberbeveiligingsprofessionals** bij de betrokken actoren vertaalt zich in het ontbreken van een instrument voor communicatie tussen werkgevers, opleiders en beleidsmakers, in het onvermogen om de lacunes op de arbeidsmarkt voor cyberbeveiliging te meten en te beoordelen. Voorts worden er geen onderwijs- en opleidingsprogramma's opgezet en worden voor degenen die de baan willen uitoefenen, geen loopbaantrajecten uitgestippeld die

[17] Cybersecurity Higher Education Database (CyberHEAD).

[18] Slechts 19 % van de ICT-specialisten in de EU is vrouw, Digital Economy and Society Index (DESI) 2022 | Shaping Europe's digital future (europa.eu). Voor vrouwelijk cyberbeveiligingspersoneel in de Unie zijn geen cijfers beschikbaar.

[19] Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030, waarbij een monitoring- en samenwerkingsmechanisme wordt ingesteld om de in het digitale kompas 2030 uiteengezette gemeenschappelijke doelstellingen en streefcijfers voor de digitale transformatie van Europa, ook op het gebied van vaardigheden, te verwezenlijken.

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

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

[22] SME definition (europa.eu).

[23] ENISA Threat Landscape 2022 – Enisa (europa.eu).

beantwoorden aan de beleids- en marktbehoeften. De **bij- en omscholing** van arbeidskrachten is in grote mate afhankelijk van cyberbeveiligingsopleidingen en -certificaten, die doorgaans door particuliere actoren worden aangeboden. Voor arbeidskrachten is het echter lastig om een beeld te krijgen van de kwaliteit van de aangeboden cyberbeveiligingsopleidingen en de bijbehorende afgegeven certificaten.

Hoewel onderwijs, opleiding en loopbaanontwikkeling noodzakelijk zijn om de aanbodzijde van de arbeidsmarkt te versterken, wordt de rol van de **vraagzijde** bij de opleiding van de beroepsbevolking en de aanpassing aan de ontwikkelingen op de arbeidsmarkt momenteel onderschat. Het ontbreekt werkgevers uit het bedrijfsleven en de publieke sector aan gemeenschappelijke fora en plaatsen waar zij ideeën kunnen bundelen over manieren waarop arbeidskrachten het best kunnen worden opgeleid, en kunnen bespreken hoe **vaardigheden beter kunnen worden beoordeeld**, met name tijdens aanwervingsprocedures. De meest gevraagde **harde vaardigheden** zijn weliswaar cyberbeveiligingsvaardigheden[24], zoals softwareontwikkeling of cloudcomputing[25], maar **transversale vaardigheden** worden nog altijd ten onrechte geringschat. Kritisch denken en analyseren, probleemoplossing en zelfbeheer zijn vaardigheidsgroepen die steeds meer door werkgevers worden gevraagd[26] en tot 2025 aan belang zullen winnen[27].

Er bestaan al veel publieke en particuliere investeringsinitiatieven op het gebied van cyberbeveiligingsvaardigheden, en de EU **financiert** via verschillende instrumenten op ruime schaal projecten[28]. Het aanhoudende tekort aan vaardigheden in de EU doet echter vragen rijzen over de zichtbaarheid en impact van die initiatieven en duidt erop dat deze niet stelselmatig aansluiten bij de marktbehoeften, die dringend op EU-niveau in kaart moeten worden gebracht. Daarnaast leiden verschillende financieringsbronnen tot overlapping, waardoor niet kan worden opgeschaald en geen reëel effect kan worden gesorteerd. Bovendien kunnen degenen die de investering nodig hebben, niet altijd de bronnen vinden die het best bij hun behoeften aansluiten.

Belanghebbenden hebben getracht het complexe en veelzijdige probleem van het tekort aan cyberbeveiligingsvaardigheden aan te pakken: het EU-Agentschap voor cyberbeveiliging (Enisa) heeft instrumenten inzake rolprofielen en hoger onderwijs ontwikkeld[29]; het Europees Kenniscentrum voor cyberbeveiliging (ECCC)[30] houdt zich in een speciale werkgroep bezig met cyberbeveiligingsvaardigheden; de Europese Veiligheids- en defensieacademie (ESDC) werkt in het kader van het gemeenschappelijk veiligheids- en defensiebeleid aan de cyberbeveiligingsvaardigheden van militair en burgerpersoneel[31]; particuliere organisaties

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

[25] ISACA State of Cyber Security 2022 infographic.

[26] Zoals het Cedefop-instrument: Skills-OVATE | Cedefop (europa.eu).

[27] The Future of Jobs Report, Wereld Economisch Forum, oktober 2020.

[28] Bijvoorbeeld: Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project (gefinancierd door het Erasmus+-programma), projecten ter ondersteuning van het Kenniscentrum voor cyberbeveiliging (ECHO, Concordia, CyberSec4Europe, Sparta (gefinancierd door Horizon 2020), Cybersecpro (gefinancierd door het programma Digitaal Europa)).

[29] Met name: Europees kader voor cyberbeveiligingsvaardigheden (ECSF), Cybersecurity Higher Education Database (CyberHEAD), Cyber Exercise Platform (CEP), European Cyber Security Challenge, Europese maand van de cyberbeveiliging.

[30] Verordening (EU) 2021/887 van het Europees Parlement en de Raad van 20 mei 2021 tot oprichting van het Europees kenniscentrum voor industrie, technologie en onderzoek op het gebied van cyberbeveiliging en het netwerk van nationale coördinatiecentra.

[31] Met name: platform voor onderwijs, opleiding, evaluatie en oefeningen op cybergebied (ETEE).

proberen de kwestie het hoofd te bieden[32], en de cyberbeveiligingscertificeringssector ontwikkelt een routekaart en opleidingen om de lacunes op het gebied van vaardigheden aan te pakken[33]. Ook de lidstaten leggen zich op de kwestie toe in het kader van diverse initiatieven, variërend van regelgeving[34] tot de oprichting van academies voor cyberbeveiligingsvaardigheden[35], cybercampussen[36] of kenniscentra op het gebied van cybercriminaliteit[37], tot publiek-private partnerschappen[38]. Bij de werkzaamheden van al deze belanghebbenden ontbreekt het echter vaak aan coördinatie en synergieën, en hun potentieel om een aanzienlijk verschil te maken op de arbeidsmarkt is niet verwezenlijkt, zoals blijkt uit het groeiende tekort aan cyberbeveiligingspersoneel in de EU. Er is tevens behoefte aan meer synergieën tussen cybergemeenschappen, aangezien de vaardigheden die nodig zijn om cyberbeveiliging te handhaven, **cybercriminaliteit** te bestrijden of **cyberdefensierespons** op te bouwen, vaak van vergelijkbare aard zijn.

Ten slotte beschikt de EU momenteel over beperkte middelen om **de stand en de ontwikkeling van de arbeidsmarkt voor cyberbeveiliging** en van de vaardigheden van de beroepsbevolking op dit gebied te beoordelen. De lidstaten en instellingen, organen en instanties van de Unie baseren zich ofwel op door private entiteiten verzamelde gegevens, ofwel op een bredere reeks door de EU – met name Eurostat[39] en het Europees Centrum voor de ontwikkeling van de beroepsopleiding (Cedefop)[40] – verzamelde gegevens over ICT-professionals. De EU heeft, kortom, een onvolledig en versnipperd beeld van haar behoeften, waardoor zij niet in staat is een globale visie op de stand van de cyberbeveiligingsarbeidsmarkt te bestendigen.

3. Een gecoördineerde respons voor de hele EU: de academie voor cyberbeveiligingsvaardigheden

3.1. Doel

Om de uitdagingen op het gebied van cyberbeveiligingsvaardigheden het hoofd te bieden en de lacunes op de arbeidsmarkt op te vullen, stelt de Commissie een **academie voor cyberbeveiligingsvaardigheden** voor, zoals aangekondigd door de voorzitter van de Europese Commissie in haar intentieverklaring bij de Staat van de Unie 2022[41, 42] en in het kader van het Europees Jaar van de Vaardigheden.

De academie voor cyberbeveiligingsvaardigheden (in het kort: "de academie") heeft tot doel een **centraal toegangspunt en synergieën** te creëren voor het onderwijs- en opleidingsaanbod op het gebied van cyberbeveiliging, alsook voor

[32] Bijvoorbeeld werkgroep 5 van de Europese organisatie voor cyberbeveiliging (ECSO) over "Onderwijs, opleiding, bewustmaking, cybertestvoorzieningen, menselijke factoren" en de organisatie DIGITALEUROPE.

[33] Bijvoorbeeld SANS Institute, (ISC)², Isaca.

[34] Bijvoorbeeld in nationale strategieën voor onderwijs of cyberbeveiliging.

[35] Bijvoorbeeld C-Academy in Portugal.

[36] Bijvoorbeeld cybercampussen in Frankrijk.

[37] Bijvoorbeeld het Litouwse kenniscentrum op het gebied van cybercriminaliteit voor opleiding, onderzoek en onderwijs in Litouwen (L3CE).

[38] Bijvoorbeeld het scholingsinititief op het gebied van cyberbeveiligingsvaardigheden van Microsoft.

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

[40] Zoals het Cedefop-instrument: Skills-OVATE | Cedefop (europa.eu).

[41] Intentieverklaring bij de Staat van de Europese Unie 2022 aan voorzitter Roberta Metsola en premier Petr Fiala.

[42] Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

financieringsmogelijkheden en specifieke maatregelen ter ondersteuning van de ontwikkeling van cyberbeveiligingsvaardigheden. De academie zal initiatieven van belanghebbenden zodanig opschalen dat er een kritische massa wordt bereikt, teneinde een verschil te maken op de arbeidsmarkt – ook met betrekking tot defensie. De activiteiten zouden op gemeenschappelijke doelstellingen en kernprestatie-indicatoren worden afgestemd om een groter effect te sorteren.

De academie zal vooral gericht zijn op de scholing van **cyberbeveiligingsprofessionals**. De activiteit van de academie wordt meegenomen in het EU-beleid inzake cyberbeveiliging, maar ook in onderwijs en een leven lang leren, en vormt een aanvulling op de twee aanbevelingen van de Raad over digitaal onderwijs en digitale vaardigheden die de Commissie tegelijk met deze mededeling heeft voorgesteld[43].

De academie heeft vier pijlers: 1) bevorderen van **kennisopbouw via onderwijs en opleiding** door een gemeenschappelijk kader voor rolprofielen op het gebied van cyberbeveiliging en bijbehorende vaardigheden uit te werken, het Europese aanbod aan onderwijs en opleidingen te verbeteren om aan de behoeften te voldoen, loopbaantrajecten uit te stippelen en ruchtbaarheid te geven aan en duidelijkheid te verschaffen over cyberbeveiligingsopleidingen en -certificeringen om het arbeidsaanbod te vergroten; 2) zorgen voor een betere benutting en grotere zichtbaarheid van de beschikbare **financieringsmogelijkheden** voor activiteiten met betrekking tot vaardigheden, om de impact ervan te maximaliseren; 3) aansporen van belanghebbenden om **actie te ondernemen**, en 4) vaststellen van indicatoren om de **marktevolutie te monitoren** en de doeltreffendheid van maatregelen te kunnen beoordelen.

De oprichting van de academie wordt ondersteund met 10 miljoen EUR uit het programma Digitaal Europa[44].

3.2.Beheer van de academie

Om ten slotte te voorzien in infrastructuur die als **centraal toegangspunt** dient om de samenwerking tussen de academische wereld, opleidingsaanbieders en het bedrijfsleven te bevorderen, waar vraag- en aanbodzijde van het EU-cyberbeveiligingsecosysteem elkaar kunnen vinden en kunnen worden opgeleid, zou de academie de vorm van een **Europees consortium voor digitale infrastructuur (EDIC)**[45] kunnen aannemen. Dit instrument zou de lidstaten in staat stellen gezamenlijk te werken aan het opvullen van de lacunes op het gebied van cyberbeveiligingsvaardigheden, nauw samen te werken met de Commissie, Enisa en het Europees Kenniscentrum voor cyberbeveiliging (ECCC), in overeenstemming met hun mandaten en bevoegdheden, en alle relevante belanghebbenden bij elkaar te brengen, maar ook Europese, nationale en particuliere investeringen te richten op een gemeenschappelijk doel. In dit verband wordt belangstellende lidstaten verzocht om uiterlijk 30 mei 2023 bij de Commissie een voorafgaande kennisgeving van hun toekomstige aanvraag voor een dergelijk EDIC in te dienen. Deze vrijwillige voorafgaande kennisgeving zou de Commissie in staat stellen in een vroeg stadium opmerkingen te maken over het ontwerp van de EDIC-aanvraag, zodat deze sneller kan worden uitgewerkt en formeel kan worden ingediend. Gedurende het gehele proces en voor zover de lidstaten daarom verzoeken, zal de Commissie, als een

[43] Voorstellen voor aanbevelingen van de Raad over de essentiële randvoorwaarden voor succesvol digitaal onderwijs en digitale opleiding en over de verbetering van het aanbod van digitale vaardigheden in onderwijs en opleiding.

[44] Verordening (EU) 2021/694 van het Europees Parlement en de Raad van 29 april 2021 tot vaststelling van het programma Digitaal Europa en tot intrekking van Besluit (EU) 2015/2240.

[45] Zie voor de oprichting van EDIC's Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030, artikelen 13 en volgende.

incubator van meerlandenprojecten, de voorbereiding van de EDIC-aanvraag faciliteren. Na een positieve beoordeling van de aanvraag door de Commissie en na de goedkeuring door het programmacomité voor het digitale decennium zal dan een besluit tot oprichting van het EDIC worden genomen, waarna bijstand wordt verleend bij de coördinatie van de uitvoering van het EDIC[46].

In de tussentijd, en terwijl het EDIC formeel wordt opgericht, zal de Commissie een virtueel centraal toegangspunt instellen door haar **platform voor digitale vaardigheden en banen**[47] te versterken met de steun van het project European Cybersecurity Community Support (ECCO)[48].

Enisa zal in overeenstemming met zijn doelstellingen een bijdrage leveren aan de uitvoering van de academie[49], met name via bijstand voor onderwijs en opleiding op het gebied van cyberbeveiliging, en neemt daarbij de rapportageverplichtingen uit hoofde van de NIS2-richtlijn[50] in aanmerking. Het **ECCC** zal zijn werkzaamheden in overeenstemming met zijn strategische agenda verrichten om de uitvoering van de academie voor cyberbeveiligingsvaardigheden te ondersteunen. Het zal met name strategische doelstelling 3 (cyberbeveiliging) van het programma Digitaal Europa uitvoeren en krijgt daarbij steun van de Commissie en de lidstaten via de **nationale coördinatiecentra (NCC's)**. In voorkomend geval wordt een beroep gedaan op de uit hoofde van de NIS2-richtlijn[51] opgerichte **samenwerkingsgroep**. Tot slot moeten de krachten met het **bedrijfsleven** en de **academische wereld** worden gebundeld om te beantwoorden aan het doel van de academie om de lacunes op het gebied van cyberbeveiligingsvaardigheden op te vullen.

4. Kennisopbouw en opleiding: vaststellen van een gemeenschappelijke EU-aanpak voor opleidingen op het gebied van cyberbeveiliging

In het kader van de pijler kennisopbouw en opleiding van de academie voor cyberbeveiligingsvaardigheden wordt een gestructureerde aanpak ontwikkeld met als duidelijk doel het **aantal** personen met cyberbeveiligingsvaardigheden in de EU te verhogen, opleidingen beter af te stemmen op de **behoeften van de markt** en zichtbaarheid te geven aan **loopbaantrajecten**.

---

[46] Ibid., artikel 12.

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

[48] Zie European Cybersecurity Competence Centre and Network:new EU-funded project to support the Cyber Community (europa.eu). In december 2022 ondertekende de Europese Commissie een contract van 3 miljoen EUR ter ondersteuning van de EU-cybergemeenschap in het kader van het Europees Kenniscentrum voor cyberbeveiliging. Dit project zal bijdragen tot de doelstellingen van de EU inzake gemeenschaps- en capaciteitsopbouw wat betreft onderzoek, innovatie, invoering en industriële basis op het gebied van cyberbeveiliging.

[49] "Enisa ondersteunt de capaciteitsopbouw en de paraatheid in de hele Unie door de instellingen, organen en instanties van de Unie, alsmede de lidstaten en publieke en particuliere belanghebbenden bij te staan teneinde [...] vaardigheden en bekwaamheden op het gebied van cyberbeveiliging te ontwikkelen." Artikel 4, lid 3, van de cyberbeveiligingsverordening.

[50] Artikel 18 van de NIS2-richtlijn.

[51] Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn).

4.1. Dezelfde taal spreken: een gemeenschappelijke aanpak van rolprofielen op het gebied van cyberbeveiliging en bijbehorende vaardigheden

Enisa heeft in de context van het Europees kader voor cyberbeveiligingsvaardigheden (**ECSF**)[52] al aan de definiëring van rolprofielen van cyberbeveiligingsprofessionals gewerkt. De academie moet dit kader als basis gebruiken om relevante vaardigheden vast te stellen en te beoordelen, de ontwikkeling van de lacunes op het gebied van vaardigheden te monitoren en aanwijzingen te geven omtrent de nieuwe behoeften. Voor elke cyberbeveiligingsrol van het ECSF wordt een reeks toepasselijke e-vaardigheden van het Europees kader voor e-vaardigheden[53] opgenomen in de profielbeschrijving[54].

Enisa zal daarom het ECSF evalueren en **veranderende behoeften en lacunes op het gebied van vaardigheden** bij cyberbeveiligingspersoneel **in kaart brengen**, ook met behulp van geavanceerde instrumenten (bv. artificiële intelligentie, big data[55], datamining). Daarbij werkt Enisa onder leiding van het EDIC, zodra het is opgericht, het ECCC – samen met de NCC's – , de Commissie, het ECCO-project en marktdeelnemers[56]. Wat cyberdefensiepersoneel betreft, zal Enisa naar behoren rekening houden met de werkzaamheden van de ESDC. Evenzo zal Enisa op het vlak van de bestrijding van cybercriminaliteit de activiteiten van het Agentschap van de EU voor opleiding op het gebied van rechtshandhaving (Cepol) en Europol in aanmerking nemen om een analyse op te stellen van de operationele opleidingsbehoeften[57] op het gebied van cyberaanvallen.

Het ECSF zal binnen de academie regelmatig worden aangevuld en geëvalueerd gedurende een tweejarige cyclus. Daarnaast zullen de Commissie en de Europese Dienst voor extern optreden waar nodig specifieke profielen en bijbehorende vaardigheden voor sectoren helpen vaststellen, met steun van EU-agentschappen en -organen zoals de ESDC[58], Europol en Cepol[59].

Er worden ook verbanden gelegd tussen het ECSF en de relevante instrumenten van het EU-werkgelegenheidsbeleid[60]. Met name worden de ECSF-functieprofielen en de bijbehorende vaardigheden in de **ESCO-classificatie** opgenomen. Hierdoor worden beroepen en vaardigheden op het gebied van cyberbeveiliging beter geclassificeerd en aan elkaar gekoppeld, waardoor mensen zich gemakkelijker kunnen bij- en omscholen en vaardigheden

---

[52] European Cybersecurity Skills Framework (ECSF) – Enisa (europa.eu) Het ECSF ondersteunt de vaststelling en formulering van taken, competenties, vaardigheden en kennis die verband houden met de rol van Europese cyberbeveiligingsprofessionals. Het vat alle rollen in verband met cyberbeveiliging samen in profielen, die afzonderlijk worden geanalyseerd op hun respectieve verantwoordelijkheden, vaardigheden, synergieën en onderlinge afhankelijkheden.

[53] European e-Competence Framework (e-CF) | ESCO (europa.eu) Het Europees kader voor e-vaardigheden (e-CF) zorgt voor samenhang in de context van ICT-kwalificaties en andere voor de sector relevante kaders, waaronder DigComp.

[54] Zie in dit verband User Manual – European Cybersecurity Skills Framework (ECSF) – september 2022.

[55] Zie bijvoorbeeld Skills-OVATE, ontwikkeld door Cedefop.

[56] Enisa zal verder gebruikmaken van de resultaten van andere door de EU gefinancierde projecten (bv. REWIRE, Data Space For Skills (DS4s), CyberSecPro, Concordia) en methoden die voortvloeien uit soortgelijke initiatieven (bv. OESO-verslag getiteld "Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States" van 21 maart 2023) om in de toekomst te kunnen zorgen voor een actuele visie op de behoeften in een omgeving waar de vraag voortdurend evolueert.

[57] CEPOL Operational Training Needs Assessment (OTNA).

[58] Zie in dit verband Gezamenlijke mededeling aan het Europees Parlement en de Raad, Het EU-beleid op het gebied van cyberdefensie, JOIN(2022) 49 final.

[59] In dit verband zal aandacht uitgaan naar de afronding van het kader voor opleidingscompetenties op het gebied van cybercriminaliteit (Cybercrime Training Competency Framework, TCF), dat momenteel wordt ontwikkeld.

[60] Zoals de Europese classificatie van vaardigheden, competenties, kwalificaties en beroepen (ESCO), Europass en het Europees samenwerkingsnetwerk van diensten voor arbeidsvoorziening (EURES).

verder afgestemd worden op de vraag van de arbeidsmarkt alsook grensoverschrijdende mobiliteit wordt ondersteund.

4.2. Bevorderen van samenwerking bij de opzet van onderwijs- en opleidingsprogramma's op het gebied van cyberbeveiliging

Zodra het EDIC is opgericht, moet de academie steun van de lidstaten ontvangen om de **referentielocatie in Europa te worden wat betreft opzet en aanbod van cyberbeveiligingsopleidingen** die gericht zijn op de meest gevraagde vaardigheden. Zij moet opleidingen op de werkplek en stagemogelijkheden aanbieden voor start-ups en kmo's alsook voor overheidsdiensten in innovatieve bedrijven op het gebied van cyberbeveiliging en kenniscentra voor cyberbeveiliging. Het EDIC moet bij de opzet van dergelijke opleidingen samenwerken met alle relevante belanghebbenden, waaronder het bedrijfsleven, en voortbouwen op projecten zoals **CyberSecPro**[61], dat door het programma Digitaal Europa wordt gefinancierd en 17 instellingen voor hoger onderwijs en 13 beveiligingsbedrijven uit 16 lidstaten bijeenbrengt om uit te groeien tot de beste praktijk voor alle opleidingsprogramma's op het gebied van cyberbeveiliging.

De academie zal met alle relevante belanghebbenden samenwerken om **de jongere generaties te enthousiasmeren** voor een loopbaan in cyberbeveiliging. In overeenstemming met het voorstel voor een aanbeveling van de Raad over de verbetering van het aanbod van digitale vaardigheden in onderwijs en opleiding moeten de lidstaten maatregelen vaststellen en versterken om gespecialiseerde leerkrachten en opleiders aan te werven en op te leiden en de verwerving van cyberbeveiligingsvaardigheden te vergemakkelijken, onder meer door middel van leer-werktrajecten. De integratie van cyberbeveiliging in onderwijs- en opleidingsprogramma's moet worden aangemoedigd: daarbij moet de toegankelijkheid van die programma's worden gewaarborgd, moet het aanbod aan **leer-werktrajecten** en stages verder worden ontwikkeld, moeten innovatieve benaderingen zoals serious games en gedeelde simulatieplatforms worden bevorderd, onderdompelingsweken voor cyberbeveiligingsfuncties worden georganiseerd en niet-technische rolprofielen worden toegelicht. Ook moet steun worden verleend om moeilijk te bereiken groepen, zoals jongeren met een handicap, in afgelegen regio's of plattelandsgebieden, en andere minderheidsgroepen te laten deelnemen aan deze leermogelijkheden op het gebied van cyberbeveiliging.

De Commissie blijft steun verlenen voor de ontwikkeling van microcredentials en beroepsonderwijs- en opleidingsprogramma's. Met name worden **gezamenlijke bachelor- en masterprogramma's, gezamenlijke cursussen of modules die kunnen leiden tot microcredentials,** en **gecombineerde intensieve programma's**[62] over alle thema's, waaronder **cyberbeveiliging**, in het kader van Erasmus+ verder gefinancierd. De verdere uitrol van het **initiatief "Europese universiteiten"**[63] en van **kenniscentra voor beroepsopleiding**[64] wordt ook ondersteund om nauwere samenwerking tussen hoger onderwijs en relevante instellingen voor beroepsonderwijs- en opleiding door heel Europa te

[61] CyberSecPro zal bijvoorbeeld zorgen voor een analyse van de programma's en (zomer)cursussen op het gebied van cyberbeveiliging die aan universiteiten worden aangeboden, en van de gebruikte tabellen van het Europese studiepuntensysteem (ECTS). Voorts moet het streefcijfer van meer dan 530 stagiairs in de driejarige periode wordt gehaald en wordt een opleiding gegeven aan externe personen uit diverse bedrijfstakken en sectoren.

[62] Bij gecombineerde intensieve programma's wordt online-onderwijs gecombineerd met een korte periode van fysieke mobiliteit.

[63] Initiatief "Europese universiteiten" |European Education Area (europa.eu).

[64] Kenniscentra voor beroepsopleiding |Erasmus+ (europa.eu).

stimuleren. Deze doelstelling van nauwere samenwerking wordt geschraagd door financieringsprogramma's van de EU, zoals Erasmus+ en het programma Digitaal Europa, en door EU-middelen voor de ontwikkeling van **individuele leerrekeningen**[65].

Om de samenwerking op nationaal niveau tussen de academische wereld en aanbieders van opleidingen op het gebied van cyberbeveiligingsvaardigheden enerzijds en werkgevers uit de particuliere en publieke sector anderzijds te vergemakkelijken en synergieën tussen de publieke en de particuliere sector te bevorderen, wordt de NCC's verzocht na te gaan of het mogelijk is om **cybercampussen** in de lidstaten op te richten. De cybercampussen zouden fungeren als nationale expertisecentra voor de cyberbeveiligingsgemeenschap, en de academie zou hun netwerkactiviteiten en de verdere coördinatie van hun werkzaamheden ondersteunen.

Enisa zal zijn opleidingsaanbod op het gebied van cyberbeveiliging ook verbeteren door zijn **cursuscatalogus**[66] op de ECSF-profielen af te stemmen en opleidingsmodules per profiel uit te werken, zodat het opleidingsaanbod van de lidstaten mogelijk groter wordt. Enisa zal daarnaast zijn **"Train the trainer"-programma**[67] uitbreiden met het oog op de professionele behoeften van de instellingen, organen en instanties van de Unie, overheidsautoriteiten van de lidstaten en **publieke en particuliere kritieke aanbieders** binnen het toepassingsgebied van de NIS2-richtlijn.

Bovendien zullen andere EU-agentschappen en -organen hun opleidingsaanbod op het gebied van cyberbeveiliging versterken. Bij de uitvoering van het EU-beleid inzake cyberdefensie zal de **ESDC** bijvoorbeeld een nieuwe reeks cyberbeveiligingscursussen ontwikkelen en een aantal van haar huidige cursussen afstemmen op het ECSF. Deze cursussen zullen leiden tot de certificering van leerresultaten[68]. De ESDC zal in samenwerking met de Commissie onderzoeken of het mogelijk is om certificaten op te nemen in de EUeID-portemonnee. Zij zal verder ingaan op de mogelijke beoordeling van vaardighedenmechanismen op grond waarvan de certificaten worden afgegeven. Op het gebied van de bestrijding van cybercriminaliteit zal tevens worden gestreefd naar nauwe banden met de **Cepol Cybercrime Academy**[69], met het oog op synergieën en complementariteit bij de opzet en uitvoering van opleidingsprogramma's.

4.3. Synergieën creëren en ruchtbaarheid geven aan cyberbeveiligingsopleidingen en -certificering in de lidstaten

De academie moet aandacht besteden aan de zichtbaarheid van en synergieën tussen opleiding en certificering. Dit zou de civiele, defensie-, rechtshandhavings- en diplomatieke cybergemeenschappen ten goede komen, aangezien alle sectoren in veel gevallen behoefte hebben aan dezelfde expertise, die gebaseerd is op vergelijkbare leerprogramma's en -resultaten.

---

[65] In overeenstemming met de aanbeveling van de Raad van 16 juni 2022 inzake individuele leerrekeningen.

[66] Training Courses – Enisa (europa.eu).

[67] Train the trainer programme – Enisa (europa.eu).

[68] In overeenstemming met artikel 20, lid 4, van Besluit (GBVB) 2020/1515 van de Raad van 19 oktober 2020 tot oprichting van een Europese Veiligheids- en defensieacademie en tot intrekking van Besluit (GBVB) 2016/2382.

[69] De Cepol Cybercrime Academy is in 2019 opgericht om te voorzien in een geavanceerd platform ter verbetering van de kennis over cybercriminaliteit en de cybercapaciteiten in Europa.

De academie zou een **centraal toegangspunt** bieden voor mensen die belangstelling hebben voor een cyberbeveiligingsloopbaan. Dit wordt op korte termijn verwezenlijkt door het **platform voor digitale vaardigheden en banen** van de Commissie uit te breiden met steun van het ECCO-project. In een speciale sectie inzake cyberbeveiligingsloopbanen worden bestaande instrumenten – zoals programma's voor hoger onderwijs of opleidingsmogelijkheden, waaronder cursussen die tot microcredentials leiden en programma's voor beroepsonderwijs en -opleiding – gekoppeld aan vacatures. Hiertoe worden in het platform lopende werkzaamheden en initiatieven vermeld of geïntegreerd, bv. de werkzaamheden en initiatieven van Enisa, dat in samenwerking met de academische wereld **onderwijsinstellingen** die cyberbeveiligingsprogramma's aanbieden, **in kaart heeft gebracht**. Met steun van de NCC's worden in dit verband verdere verbeteringen aangebracht. Daarnaast zal Enisa, met steun van de NCC's, de Commissie en het ECCO-project en in samenwerking met entiteiten die certificaten afgeven, twee **registers van bestaande opleidingen uit publieke en particuliere sectoren en van cyberbeveiligingscertificeringen** ontwikkelen en consolideren, waarbij ook op andere relevante initiatieven wordt voortgebouwd[70]. Deze worden ook geïntegreerd in het centrale toegangspunt van het platform voor digitale vaardigheden en banen. Deze werkzaamheden komen ook ten goede aan de NCC's, die met name tot taak hebben onderwijsprogramma's op het gebied van cyberbeveiliging te bevorderen en te verspreiden[71].

Aan professionals moet ook de garantie worden geboden dat de opleidingen die zij volgen de vereiste kwaliteit hebben. In dit verband zal Enisa een **proefproject** opzetten om onderzoek te doen naar een Europese attestregeling voor cyberbeveiligingsvaardigheden.

Daarnaast is het essentieel om vaardigheden en opleidingen te identificeren en aan een functieprofiel te verbinden, maar moet ook worden gegarandeerd dat cyberbeveiligingsdiensten over de nodige bekwaamheid, deskundigheid en ervaring beschikken. Dit geldt met name voor aanbieders van beheerde beveiligingsdiensten op gebieden als respons op incidenten, penetratietests en beveiligingsaudits en -consultancy. In de NIS2-richtlijn en het voorstel voor de verordening cybersolidariteit zijn specifieke taken vastgesteld voor dergelijke aanbieders van beheerde beveiligingsdiensten. De Commissie stelt daarom ook een **gerichte wijziging van de cyberbeveiligingsverordening**[72] voor om certificeringsregelingen voor beheerde beveiligingsdiensten op EU-niveau mogelijk te maken. Dergelijke certificeringsregelingen moeten er onder meer voor zorgen dat deze diensten worden verleend door personeel met een zeer hoge mate van technische kennis en bekwaamheid op de relevante gebieden.

Kwaliteitsborging en erkenningsmechanismen voor microcredentials[73] bevorderen de transparantie, vergelijkbaarheid en overdraagbaarheid van leerresultaten. In overeenstemming

[70] Bijvoorbeeld de W4C Academy - Women4Cyber of het Global Cybercrime Certification project voor rechtshandhavings- en justitiële autoriteiten.

[71] "1. De nationale coördinatiecentra verrichten de volgende taken: [...] g) onverlet de bevoegdheden van de lidstaten op het gebied van onderwijs en rekening houdend met de betreffende taken van Enisa, overleggen met de nationale autoriteiten over mogelijke bijdragen aan de bevordering en verspreiding van onderwijsprogramma's op het gebied van cyberbeveiliging" (artikel 7, lid 1, punt g), van de ECCC-verordening). Zie ook de hiermee samenhangende overweging 28.

[72] Verordening (EU) 2019/881 van het Europees Parlement en de Raad van 17 april 2019 inzake Enisa (het Agentschap van de Europese Unie voor cyberbeveiliging), en inzake de certificering van de cyberbeveiliging van informatie- en communicatietechnologie en tot intrekking van Verordening (EU) nr. 526/2013 (de cyberbeveiligingsverordening).

[73] Bijvoorbeeld registratie of certificaten van bij korte opleidingen behaalde leerresultaten.

met de aanbeveling van de Raad betreffende een Europese benadering van microcredentials[74] worden de lidstaten aangemoedigd om microcredentials voor cyberbeveiliging op te nemen in hun nationale kwalificatiekaders. Op die manier kunnen zij de microcredentials voor cyberbeveiliging koppelen aan het Europees kwalificatiekader[75]. Via de Europese digitale credentials voor leerinfrastructuur kunnen digitaal ondertekende cyberbeveiligingskwalificaties en microcredentials van particulieren worden afgegeven. Deze bevatten waardevolle gegevens, onder meer over leerresultaten op het gebied van cyberbeveiliging, en kunnen in de toekomstige **digitale EUeID-portemonnee**[76] worden opgeslagen.

Maatregelen in het kader van de academie

Lidstaten en bedrijfsleven

- Ondersteunen van de ontwikkeling en erkenning van **microcredentials** op het gebied van cyberbeveiliging, in overeenstemming met de aanbeveling van de Raad betreffende een Europese benadering van microcredentials.
- Cyberbeveiligingkwalificaties, met inbegrip van microcredentials, opnemen in **nationale kwalificatiekaders**.
- **Mogelijkheden voor leren op de werkplek** aanbieden via leer-werktrajecten voor mensen die deelnemen aan initiatieven voor de ontwikkeling van cyberbeveiligingsvaardigheden.

Commissie

- Op korte termijn – uiterlijk eind 2023 – een **centraal toegangspunt** creëren voor cyberbeveiligingsprogramma's, bestaande opleidingen en cyberbeveiligingscertificeringen via het **platform voor digitale vaardigheden en banen**.
- Het voorstel van 18 april 2023 tot wijziging van de **cyberbeveiligingsverordening**, om de certificering van aanbieders van beheerde beveiligingsdiensten mogelijk te maken.

Organen en instanties van de Unie

- Uiterlijk eind 2023 het **ECSF** vaststellen als gemeenschappelijke aanpak voor rolprofielen op het gebied van cyberbeveiliging en bijbehorende vaardigheden.
- Enisa zal in het tweede kwartaal van 2023 beginnen met de opzet van een proefproject voor de invoering van een **Europese attestregeling** voor cyberbeveiligingsvaardigheden.
- Enisa moet uiterlijk eind 2023 zijn **cursuscatalogus** herzien en zijn **"Train the trainer"-programma** openstellen voor publieke en particuliere kritieke aanbieders.
- Medio 2023 de **afstemming van de ESDC-leerprogramma's op het ECSF** afronden.

[74] Aanbeveling van de Raad betreffende een Europese benadering van microcredentials voor een leven lang leren en inzetbaarheid op de arbeidsmarkt.

[75] Aanbeveling van de Raad van 22 mei 2017 inzake het Europees kwalificatiekader voor een leven lang leren en tot intrekking van de aanbeveling van het Europees Parlement en de Raad van 23 april 2008 tot vaststelling van een Europees kwalificatiekader voor een leven lang leren.

[76] Voorstel voor een verordening van het Europees Parlement en de Raad tot wijziging van Verordening (EU) nr. 910/2014 betreffende een Europees kader voor een digitale identiteit.

5. Betrokkenheid van belanghebbenden: toezeggingen om de lacunes op het gebied van cyberbeveiligingsvaardigheden op te vullen

Binnen de academie zal de betrokkenheid van belanghebbenden op gecoördineerde wijze worden ontwikkeld om de lacunes op het gebied van cyberbeveiligingsvaardigheden aan te pakken. Doel is de toezeggingen van de verschillende belanghebbenden een maximale zichtbaarheid en impact te verlenen om de lacunes op het gebied van cyberbeveiligingsvaardigheden aan te pakken.

De Commissie verzoekt belanghebbenden concrete toezeggingen te doen om werknemers via gerichte acties bij en om te scholen, en daarbij zoveel mogelijk in te spelen op de vastgestelde lacunes op het gebied van cyberbeveiligingsvaardigheden. Dergelijke **toezeggingen van belanghebbenden op het gebied van cyberbeveiliging** moeten worden vermeld op het **platform voor digitale vaardigheden en banen**, op dezelfde wijze als andere digitale toezeggingen die reeds op het platform worden weergegeven. Voorts moedigt de Commissie belanghebbenden die op het platform een toezegging inzake cyberbeveiliging doen, aan om zich aan te sluiten bij het **grootschalige digitale partnerschap van het pact voor vaardigheden**[77]. Toezeggingen die in het kader van het grootschalige digitale partnerschap worden gedaan, worden bij voorkeur ingevoerd op het platform voor digitale vaardigheden en banen. Evenzo worden toezeggingen die op het platform voor digitale vaardigheden en banen zijn gedaan, bij voorkeur gemeld via het grootschalige digitale partnerschap van het pact voor vaardigheden.

De Commissie roept de lidstaten ook op **zich in te zetten voor de uitvoering van de verklaring "Women in Digital"**[78], om vrouwen aan te moedigen een actieve en prominente rol in de digitale-technologiesector op zich te nemen en een genderevenwicht in cyberbeveiligingsfuncties te bereiken. De Commissie spoort de lidstaten tevens aan synergieën met hun programma's van het **Europees Sociaal Fonds+** te ontwikkelen om de doelstelling van gendergelijkheid op het vlak van arbeidsmarktparticipatie verder te ondersteunen[79], bijvoorbeeld door **mentorschapprogramma's voor meisjes en vrouwen** op te zetten. Deze programma's kunnen de ontwikkeling van rolmodellen bevorderen – om meisjes enthousiast te maken voor cyberbeveiligingsberoepen – en tegelijkertijd gendergerelateerde stereotypen bestrijden. Dit is ook bevorderlijk voor de bij- en omscholing van vrouwen en de ontwikkeling van een gemeenschap die vrouwen kan helpen om tot de cyberbeveiligingsarbeidsmarkt toe te treden of er promotie te maken.

De lidstaten moeten **in hun nationale cyberbeveiligingsstrategieën specifieke maatregelen vaststellen om het tekort aan cyberbeveiligingsvaardigheden aan te pakken**[80], door te bepalen welke inspanningen moeten worden geleverd om de vaardigheidslacunes op te vullen en deze beter te kanaliseren, zodat zij uiteindelijk naar behoren voldoen aan hun verplichtingen uit hoofde van de NIS2-richtlijn.

Sommige lidstaten maken gebruik van **synergieën tussen civiele, defensie- en rechtshandhavingsinitiatieven**. Zij zetten bijvoorbeeld meer arbeidskrachten in met behulp

[77] New European Partnerships launched to deliver on the EU's ambitions for the Digital Decade | Shaping Europe's digital future (europa.eu), dat in het kader van het pact voor vaardigheden is opgezet om het tekort aan informatie- en communicatietechnologie (ICT) aan te pakken.

[78] EU countries commit to boost participation of women in digital | Shaping Europe's digital future (europa.eu).

[79] Verordening (EU) 2021/1057 van het Europees Parlement en de Raad van 24 juni 2021 tot oprichting van het Europees Sociaal Fonds Plus (ESF+) en tot intrekking van Verordening (EU) nr. 1296/2013, artikel 4, lid 1, punt c).

[80] NIS2-richtlijn, artikel 7, lid 2, punt f).

van de nationale dienstplicht of door gebruik te maken van cyberreservisten, d.w.z. burgers met een militaire opleiding die cyberbeveiligingsfuncties bij de strijdkrachten vervullen[81]. Door dergelijke synergieën kunnen burgers, en met name jongvolwassenen, hun vaardigheden op het gebied van cyberbeveiliging en cyberdefensie vergroten. Hetzelfde geldt voor de **bestrijding van cybercriminaliteit**, aangezien de algemene inspanningen op het gebied van cyberbeveiliging en de rechtshandhavingsactiviteiten in reactie op cyberbeveiligingsincidenten in vele gevallen gelijklopen. De Commissie is voorstander van besprekingen tussen de lidstaten over dergelijke initiatieven en verzoekt hen na te gaan op welke manier geschoolde arbeidskrachten de defensie- en civiele cyberbeveiligingsgemeenschappen het best kunnen dienen.

De Commissie zal zich beraden op voorstellen om de huidige en verwachte lacunes – die zij heeft vastgesteld bij haar evaluatie van de behoeften van de instellingen, organen en instanties van de Unie – op te vullen. Zij zal de personeelsleden met name aanmoedigen gebruik te maken van het op handen zijnde **EU-/VS-cyberbeveiligingsgenootschap**, dat in het kader van de dialoog tussen de EU en de VS is opgericht.

Maatregelen in het kader van de academie

Bedrijfsleven

- Vanaf 18 april 2023 specifieke **toezeggingen op het gebied van cyberbeveiliging** voorstellen op het platform voor digitale vaardigheden en banen.

Lidstaten

- In de **nationale cyberbeveiligingsstrategieën** specifieke maatregelen opnemen om de lacunes op het gebied van cyberbeveiligingsvaardigheden aan te pakken.

Lidstaten en bedrijfsleven

- De verklaring "Women in Digital" uitvoeren en uiterlijk in 2030 een **genderevenwicht in cyberbeveiligingsfuncties** bereiken.

6. Financiering: synergieën creëren voor een zo groot mogelijke impact van uitgaven voor de ontwikkeling van cyberbeveiligingsvaardigheden

Binnen de academie zal de impact van investeringen in cyberbeveiligingsvaardigheden worden gemaximaliseerd door een centraal toegangspunt te creëren, een betere besteding van de middelen volgens de marktbehoeften te bevorderen, het gebruik van financiering te mainstreamen, synergieën tussen verschillende instrumenten te faciliteren en dubbel werk te voorkomen[82].

6.1. Financiering afstemmen op de behoeften

Binnen de academie zal het ECCC, met steun van de Commissie, het ECCO-project en de NCC's, **informatie verzamelen over de wijze waarop EU-middelen worden ingezet voor**

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

[82] Funding opportunities (europa.eu) De ondersteuningsdiensten van het pact voor vaardigheden bieden een centraal toegangspunt voor informatie over de financiering van vaardigheden, ook voor het digitale ecosysteem. De ondersteuningsdiensten van het pact verstrekken algemene informatie over financieringsinstrumenten die niet specifiek gericht zijn op cyberbeveiligingsvaardigheden, maar de academie moet hun activiteiten wel in aanmerking nemen om dubbel werk te voorkomen.

de financiering van cyberbeveiligingsvaardigheden, en beoordelen hoe daarmee de lacunes op dit gebied worden aangepakt. Rekening houdend met deze geaggregeerde informatie zal het ECCC proberen de EU-middelen beter te kanaliseren naar de vastgestelde behoeften. Het zal maatregelen financieren om de dringendste lacunes in de beroepskrachten op het gebied van cyberbeveiliging op te vullen, onder meer in de implementatie van de desbetreffende beleidsdoelen.

6.2. Zichtbaarheid geven aan beschikbare middelen en partnerschapsinitiatieven voor cyberbeveiligingsvaardigheden

Op korte termijn wordt het **platform voor digitale vaardigheden en banen** het centrale toegangspunt voor belanghebbenden, waar alle informatie over financieringsmogelijkheden voor cyberbeveiligingsvaardigheden te vinden is.

De EU investeert in mensen en hun vaardigheden en gebruikt partnerschappen, met name met het bedrijfsleven, om actie op het gebied van bij- en omscholing te ondernemen via diverse instrumenten van de **Europese vaardighedenagenda**[83], waaronder het **pact voor vaardigheden**[84] en het **actieplan voor digitaal onderwijs**[85]. Het **programma Digitaal Europa** financiert mogelijkheden voor de verwerving van cyberbeveiligingsvaardigheden, met name via initiatieven voor meerlandenprojecten, en vormt een duidelijke aanvulling op de steun die Horizon Europa biedt voor onderzoek en innovatieve technologische oplossingen op het gebied van cyberbeveiliging. Het **Europees Defensiefonds**[86] financiert onderzoek en technologische ontwikkeling om doeltreffende cyberoperaties uit te voeren, met inbegrip van opleidingen en oefeningen[87]. **Erasmus+** blijft dergelijke initiatieven ondersteunen, onder meer via gecombineerde intensieve programma's en samenwerkingsprojecten.

De lidstaten worden aangemoedigd om de EU-middelen die zij rechtstreeks beheren, te mobiliseren om vaardigheden en banen op het gebied van cyberbeveiliging te ondersteunen. De fondsen voor het cohesiebeleid, zoals het **Europees Fonds voor regionale ontwikkeling (EFRO)** en het **ESF+** hebben in dit verband een belangrijk potentieel[88]. Ook de maatregelen in het kader van de **herstel- en veerkrachtfaciliteit**[89] en **InvestEU**[90] leveren een belangrijke bijdrage aan de verwezenlijking van de doelstellingen van de academie.

---

[83] Europese vaardighedenagenda – Werkgelegenheid, sociale zaken en inclusie – Europese Commissie (europa.eu).

[84] EU-financieringsinstrumenten voor bijscholing en omscholing – Werkgelegenheid, sociale zaken en inclusie – Europese Commissie (europa.eu).

[85] Actieplan voor digitaal onderwijs 2021-2027.

[86] Verordening (EU) 2021/697 van het Europees Parlement en de Raad van 29 april 2021 tot oprichting van het Europees Defensiefonds en tot intrekking van Verordening (EU) 2018/1092.

[87] De lidstaten zetten zich in voor gezamenlijke opleidingen en oefeningen, bijvoorbeeld door het opzetten van en deelnemen aan projecten voor permanente gestructureerde samenwerking (PESCO) op het gebied van cyberopleidingen en -oefeningen, zoals de EU-cyberacademie en innovatiehub (EU CAIH) en Federated Cyber Ranges.

[88] Artikel 3, lid 1, van Verordening (EU) 2021/1058 en artikel 4, lid 1, punt g), van Verordening (EU) 2021/1057.

[89] Het Estse herstel- en veerkrachtplan voorziet bijvoorbeeld in investeringen in digitale vaardigheden (10 miljoen EUR) om de beschikbare opleidingen voor ICT-deskundigen te herzien, de bij- en omscholing van ICT-specialisten op het gebied van cyberbeveiliging te financieren en bij te dragen tot de opzet van een proefprogramma voor de omvorming van het kwalificatiekader voor ICT-specialisten.

[90] Belanghebbenden (zoals aanbieders van opleidingen en bedrijven die hun opleidingsactiviteiten op het gebied van cyberbeveiliging willen opzetten of verbeteren) kunnen een beroep doen op de InvestEU-advieshub, die projectontwikkelaars en entiteiten technische ondersteuning – waaronder capaciteitsopbouw – biedt, en het InvestEU-portaal raadplegen.

Maatregelen in het kader van de academie

Europees Kenniscentrum voor cyberbeveiliging en Enisa

- Uiterlijk eind 2024 de bestaande EU-financiering voor cyberbeveiligingsvaardigheden **in kaart brengen** op basis van de behoeften van de markt, de **effectiviteit** ervan beoordelen en **financieringsprioriteiten** vaststellen.

Commissie

- Uiterlijk eind 2023 een **centraal toegangspunt** voor financieringsmogelijkheden voor cyberbeveiligingsvaardigheden creëren op het platform voor digitale vaardigheden en banen.

7. Meten van vooruitgang: ingebouwde verantwoordingsplicht

Binnen de academie wordt een **methodologie** ontwikkeld voor het **meten van de vooruitgang bij het opvullen van de lacunes op het gebied van cyberbeveiligingsvaardigheden**.

7.1. Vaststellen van cyberbeveiligingsindicatoren om de ontwikkeling van de arbeidsmarkt voor cyberbeveiliging te monitoren

De **index van de digitale economie en samenleving (DESI)** geeft een overzicht van indicatoren voor de digitale prestaties van Europa en volgt de vooruitgang van de EU-lidstaten. Binnen de academie voor cyberbeveiligingsvaardigheden zal Enisa in samenwerking met de Commissie en de NIS-samenwerkingsgroep[91] **indicatoren** ontwikkelen, onder meer met betrekking tot gender, om de vooruitgang van de EU-lidstaten in het aantal cyberbeveiligingsprofessionals te volgen, in overleg met relevante marktdeelnemers en de NCC's. Enisa zal voortbouwen op de DESI-methodologie[92] en waarborgen dat de indicatoren stroken met de digitale doelstellingen van de EU inzake ICT-professionals en genderevenwicht in de ICT-wereld. De Commissie zal vervolgens toewerken naar de integratie van die indicatoren in de DESI, zodat de stand van zaken op het gebied van vaardigheden en banen voor cyberbeveiliging jaarlijks kan worden getoetst.

7.2. Gegevens verzamelen en rapporteren

Enisa zal de gegevens over de indicatoren verzamelen met steun van het ECCO-project en de NCC's. Op basis van de verzamelde gegevens zal Enisa een **jaarlijks verslag** opstellen dat input levert voor het verslag over de staat van het digitale decennium[93], dat samen met de DESI wordt meegenomen in de landspecifieke analyses en aanbevelingen van het **Europees Semester**[94]. Voorts dragen de indicatoren voor cyberbeveiligingsvaardigheden bij tot het in de NIS2-richtlijn bedoelde **tweejaarlijkse verslag** van Enisa over de stand van zaken op het

[91] Op basis en ter aanvulling van de methodologie die Enisa krachtens artikel 18, lid 3, van de NIS2-richtlijn moet ontwikkelen om elke twee jaar verslag uit te brengen over de stand van zaken op het gebied van cyberbeveiliging in de Unie.

[92] Zie de methodologische toelichting bij de index van de digitale economie en samenleving (DESI) 2022, beschikbaar op The Digital Economy and Society Index (DESI) | Shaping Europe's digital future (europa.eu).

[93] Besluit (EU) 2022/2481 van het Europees Parlement en de Raad van 14 december 2022 tot vaststelling van het beleidsprogramma voor het digitale decennium tot 2030.

[94] Ibid., overweging 25.

gebied van cyberbeveiliging in de EU, dat betrekking heeft op cyberbeveiligingscapaciteiten en -bewustzijn en cyberhygiëne in de hele EU.

7.3.Ontwikkelen van kernprestatie-indicatoren (KPI's) voor cyberbeveiliging

Om het tekort aan Europese cyberbeveiligingsprofessionals weg te werken zal Enisa, in nauwe samenwerking met de Commissie en de NCC's, op basis van de methodologie van het beleidsprogramma voor het digitale decennium tot 2030 en de ervaring van de sector, KPI's aan de Commissie voorstellen. Enisa zal naar behoren rekening houden met de KPI's die de lidstaten gebruiken om hun nationale cyberbeveiligingsstrategieën te beoordelen[95].

Maatregelen in het kader van de academie

Enisa

- Uiterlijk eind 2023 **indicatoren en KPI's** voor cyberbeveiligingsvaardigheden ontwikkelen.
- Vanaf 2025 **gegevens over indicatoren verzamelen** en daarover rapporteren.

Commissie

- Toewerken naar de integratie van **cyberbeveiligingsindicatoren in de DESI** en in het **verslag over de staat van het digitale decennium**.

8. Conclusie

Deze mededeling legt de basis voor een herziening van de aanpak van de EU om de cyberbeveiligingsvaardigheden van professionals in de EU te verbeteren. Doel is de lacunes op het gebied van cyberbeveiligingsvaardigheden te verkleinen, de EU uit te rusten met de nodige arbeidskrachten om in te spelen op het voortdurend veranderende dreigingslandschap, het EU-beleid uit te voeren om de EU tegen cyberaanvallen te beschermen, maar ook de marktkansen en het concurrentievermogen te vergroten. Geschoolde arbeidskrachten op het gebied van cyberbeveiliging kunnen de **civiele, defensie-, diplomatieke en rechtshandhavingsgemeenschappen** ten goede komen en synergieën tussen die gemeenschappen bevorderen.

De Commissie roept de lidstaten en alle belanghebbenden op om de ambitie van de academie voor cyberbeveiligingsvaardigheden waar te maken.

[95] NIS2-richtlijn, artikel 7, lid 4.