Rat der
Europäischen Union

**Brüssel, den 21. April 2023**
**(OR. en)**

**8513/23**

**CYBER 93**
**TELECOM 109**
**EDUC 133**
**BUDGET 7**
**CADREFIN 52**
**EMPL 180**
**COMPET 342**
**IND 182**
**JAI 470**
**MI 313**
**POLMIL 88**

**ÜBERMITTLUNGSVERMERK**

| | |
|---|---|
| Absender: | Frau Martine DEPREZ, Direktorin, im Auftrag der Generalsekretärin der Europäischen Kommission |
| Eingangsdatum: | 19. April 2023 |
| Empfänger: | Frau Thérèse BLANCHET, Generalsekretärin des Rates der Europäischen Union |
| Nr. Komm.dok.: | COM(2023) 207 final |
| Betr.: | MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT **Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU („Akademie für Cybersicherheitskompetenzen“)** |

Die Delegationen erhalten in der Anlage das Dokument COM(2023) 207 final.

Anl.: COM(2023) 207 final

EUROPÄISCHE
KOMMISSION

Straßburg, den 18.4.2023
COM(2023) 207 final

# MITTEILUNG DER KOMMISSION AN DAS EUROPÄISCHE PARLAMENT UND DEN RAT

## Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU („Akademie für Cybersicherheitskompetenzen“)

**Schließung der Fachkräftelücke im Cybersicherheitsbereich zur Förderung der Wettbewerbsfähigkeit, des Wachstums und der Resilienz in der EU („Akademie für Cybersicherheitskompetenzen“)**

## 1. Dringlichkeit der Risikominderung durch Maßnahmen zur Beseitigung des Mangels an und der Lücken bei Cybersicherheitskompetenzen

Die Cybersicherheit ist nicht nur Teil der Sicherheit der Bürgerinnen und Bürger, der Unternehmen und der Mitgliedstaaten, sie ist auch unabdingbar, um die politische Stabilität der EU, die Stabilität ihrer Demokratien und den Wohlstand unserer Gesellschaft und unserer Unternehmen sicherzustellen. Die **Bedrohungslage** im Cybersicherheitsbereich hat sich in den letzten Jahren stark verändert; dabei zeigte sich die besorgniserregende Tendenz, dass sich immer mehr Cyberangriffe gegen militärische und zivile kritische Infrastruktur in der EU richten. Die Angreifer steigern ihre Fähigkeiten, und es gibt neue hybride und sich abzeichnende Bedrohungen wie den Einsatz von Bots und auf künstlicher Intelligenz beruhenden Methoden.[1] Insbesondere werden bei Angriffen mit Ransomware sowohl die Finanzen als auch der Ruf der Ziele regelmäßig erheblich geschädigt.[2]

Zudem betrafen viele Cybersicherheitsvorfälle die öffentliche Verwaltung und Regierungen in den Mitgliedstaaten sowie Organe, Einrichtungen und sonstige Stellen der Europäischen Union.[3] Auch das Finanzwesen[4] und das Gesundheitswesen[5], die beide tragende Säulen der Gesellschaft und der Wirtschaft sind, wurden immer wieder ins Visier genommen[6]. Aufgrund der geopolitischen Spannungen im Zusammenhang mit Russlands Angriffskrieg gegen die Ukraine haben die Cybersicherheitsbedrohungen zugenommen[7], und unsere Gesellschaft könnte destabilisiert werden. Die **Sicherheit** der EU kann nur mithilfe des **wertvollsten Guts der EU** sichergestellt werden: **mithilfe der Menschen.** Die EU braucht dringend Fachkräfte mit den Kompetenzen und Fähigkeiten, die nötig sind, um Cyberangriffe zu verhindern und zu entdecken, davon abzuschrecken, die EU und ihre wichtigste Infrastruktur dagegen zu verteidigen und ihre **Resilienz** sicherzustellen.

Die Fachkräftelücke im Cybersicherheitsbereich beeinträchtigt die **Wettbewerbsfähigkeit** und das **Wachstum** in Europa, die beide stark von der Entwicklung und Einführung

---

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

[2] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2021. Die Angreifer stützen sich auf das Modell „Ransomware als Dienstleistung“. Im Jahr 2022 wurden Unternehmen dadurch Kosten in Höhe von über 18,4 Mrd. EUR verursacht (Cybereason, 2022, Bericht über den wahren Preis von Ransomware).

[3] Siehe z. B.: gemeinsame Veröffentlichung der ENISA und des CERT-EU, JP-23-01, Sustained activity by specific threat actors, TLP:CLEAR, 15. Februar 2023.

[4] Z. B. machte Finanz-Phishing in Deutschland 90 % der zwischen dem 1. Juni 2021 und dem 31. Mai 2022 gemeldeten Fälle von Mail-Betrug aus, und es wurde ein Unternehmen im Finanzwesen angegriffen, wofür über 20 000 infizierte Geräte aus 125 Ländern zum Einsatz kamen, Die Lage der IT-Sicherheit in Deutschland 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI), 1. Januar 2023.

[5] Z. B. wurden in Frankreich öffentliche Gesundheitseinrichtungen mit Ransomware angegriffen, beispielsweise das Centre Hospitalier Sud Francilien, wobei 11 GB an personenbezogenen und medizinischen Daten sowie Personaldaten kompromittiert und vom Angreifer veröffentlicht wurden; Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d’information (ANSSI), Januar 2023.

[6] ENISA Threat Landscape 2022.

[7] Siehe auch: CERT-EU – Russia’s war on Ukraine: one year of cyber operations (europa.eu); Russische Cyberoperationen gegen die Ukraine: Erklärung des Hohen Vertreters im Namen der Europäischen Union, 10. Mai 2022; Erklärung des Hohen Vertreters im Namen der Europäischen Union zu böswilligen Cyberaktivitäten von Hackern und Hackergruppen im Zusammenhang mit der Aggression Russlands gegen die Ukraine, 19. Juli 2022.

strategischer digitaler Technologien (z. B. künstliche Intelligenz, 5G und Cloud) abhängen. Damit die EU weiterhin fortschrittliche Schlüsseltechnologien in einem globalen Umfeld bereitstellen kann, werden qualifizierte Arbeitskräfte im Cybersicherheitsbereich benötigt.

Bei der EU-Cybersicherheitspolitik wurden in den letzten Jahren erhebliche Fortschritte erzielt, um sich für diese sich wandelnde Bedrohungslage zu rüsten und sich ihr zu stellen sowie die Wettbewerbsfähigkeit der EU zu fördern; dies hat zur Annahme einer Reihe von Initiativen geführt, darunter die Cybersicherheitsstrategie der EU für die digitale Dekade[8], die überarbeitete Richtlinie über die Sicherheit von Netz- und Informationssystemen (NIS-2-Richtlinie)[9], bereichsspezifische EU-Cybersicherheitsvorschriften[10], die EU-Cyberabwehrpolitik[11], das Cyberresilienzgesetz[12] und der von der Kommission gemeinsam mit der vorliegenden Mitteilung vorgeschlagene Rechtsakt zur Cybersolidarität. Ohne die qualifizierten Arbeitskräfte, die für die Durchführung dieser Rechtsvorschriften nötig sind, können die mit ihnen verfolgten Ziele allerdings nicht erreicht werden. Im Rahmen von Initiativen zur Förderung der Entwicklung allgemeiner Kompetenzen, die für die Teilhabe an der Gesellschaft erforderlich sind, werden zwar Cybersicherheitsgrundkenntnisse der allgemeinen Bevölkerung angegangen[13], doch es werden auf nationaler Ebene und EU-Ebene sowohl im öffentlichen als auch im privaten Sektor – unter anderem in Normungsorganisationen – unbedingt kompetente Arbeitskräfte benötigt, **damit die rechtlichen und politischen Anforderungen im Cybersicherheitsbereich erfüllt werden können**.

Die Sicherheit und die Wettbewerbsfähigkeit der EU hängen somit von qualifizierten Cybersicherheitsfachkräften ab. In der EU besteht jedoch ein sehr erheblicher Mangel an qualifizierten Cybersicherheitsfachkräften, weswegen die EU, ihre Mitgliedstaaten sowie ihre Unternehmen und die Bürgerinnen und Bürger von Cybersicherheitsvorfällen bedroht sind. Im Jahr 2022 fehlten in der Europäischen Union **zwischen 260 000**[14] **und 500 000**[15] Cybersicherheitsfachkräfte, wobei der Bedarf der EU an Arbeitskräften im Cybersicherheitsbereich auf 883 000 Fachkräfte[16] geschätzt wurde; dies legt das Vorliegen eines Missverhältnisses zwischen den verfügbaren und den auf dem Arbeitsmarkt benötigten

[8] Gemeinsame Mitteilung an das Europäische Parlament und den Rat, Die Cybersicherheitsstrategie der EU für die digitale Dekade, JOIN(2020) 18 final.

[9] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

[10] Z. B. für den Finanzsektor: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011.

[11] Gemeinsame Mitteilung an das Europäische Parlament und den Rat, EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

[12] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über horizontale Cybersicherheitsanforderungen für Produkte mit digitalen Elementen und zur Änderung der Verordnung (EU) 2019/1020, COM(2022) 454 final.

[13] Zu den einschlägigen Initiativen zu allgemeinen digitalen Kompetenzen der Bevölkerung gehören: im Aktionsplan zur europäischen Säule sozialer Rechte und im digitalen Kompass festgelegtes Ziel, dass 80 % der Bevölkerung spätestens 2030 über grundlegende digitale Kompetenzen verfügen sollen, Aktionsplan für digitale Bildung 2021-2027, Instrument des Referenzrahmens für digitale Kompetenzen und Vorschlag für eine Empfehlung des Rates für eine bessere Vermittlung digitaler Kompetenzen in der allgemeinen und beruflichen Bildung.

[14] (ISC)² in: Assessing Cyber Skills on the basis of the ECSF, ENISA-Webinar, 16. Februar 2023.

[15] Laut der Europäischen Cybersicherheitsorganisation (ECSO), angegeben in: Gemeinsame Mitteilung an das Europäische Parlament und den Rat, EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

[16] (ISC)² in: Assessing Cyber Skills on the basis of the ECSF, ENISA-Webinar, 16. Februar 2023.

Kompetenzen nahe. Auch falsche Vorstellungen im Zusammenhang mit dem technischen Ruf des Berufsbildes verschärfen den Arbeitskräftemangel im Cybersicherheitsbereich, und es werden weiterhin kaum **Frauen** für den Bereich gewonnen; diese machen 20 % der Absolventinnen und Absolventen im Cybersicherheitsbereich[17] und 19 % der Fachkräfte für Informations- und Kommunikationstechnologien (IKT)[18] aus. Um Abhilfe zu schaffen, wurde im **Politikprogramm 2030 für die digitale Dekade**[19] als Ziel festgelegt, dass die Zahl der IKT-Fachkräfte bis 2030 um 20 Millionen Fachkräfte erhöht und dabei ein ausgewogeneres Geschlechterverhältnis erreicht werden soll. Außerdem werden für die Umsetzung neuer politischer Maßnahmen der EU ausreichend qualifizierte und genügend Arbeitskräfte benötigt. Beispielsweise hoben über 42 % der hochrangigen IT-Führungskräfte in der Finanzdienstleistungsbranche den Mangel an Cybersicherheitskompetenzen und -fachwissen als wesentliche Herausforderung für ihre Geschäftstätigkeit im Zusammenhang mit der Cyberabwehr und dem Vorfallmanagement hervor[20], und das zu einer Zeit, in der sie bereichsspezifische Cybersicherheitsvorschriften wie die Verordnung über die digitale operationale Resilienz im Finanzsektor umsetzen müssen.

Die zögerliche Bereitschaft der Arbeitgeber, in Humankapital zu investieren, und ihre Suche nach bereits ausgebildeten und erfahrenen Arbeitskräften tragen zusätzlich zur Anspannung auf dem Arbeitsmarkt bei.[21] Der entsprechende Mangel betrifft alle Arten von Unternehmen, auch kleine und mittlere Unternehmen (**KMU**), die 99 % aller Unternehmen in der EU ausmachen[22]. Auch **öffentliche Verwaltungen**, die in hohem Maße von Cybersicherheitsvorfällen betroffen sind und am stärksten dadurch beeinträchtigt werden, stehen vor großen Herausforderungen.[23]

Daher muss die Fachkräftelücke der EU im Cybersicherheitsbereich dringend geschlossen werden, denn die Sicherheit und die Wettbewerbsfähigkeit der EU stehen auf dem Spiel.

## 2. Mangel an Synergieeffekten und koordinierten Maßnahmen zur Schließung der Lücke bei Cybersicherheitskompetenzen

Europäische und nationale Initiativen öffentlicher und privater Einrichtungen zur Behebung der Mängel auf dem Cybersicherheitsarbeitsmarkt florieren. Allerdings sind sie verstreut und haben bislang noch nicht die „kritische Masse“ erreicht, die nötig wäre, um wirklich etwas zu bewirken.

Zunächst einmal gibt es derzeit nur begrenzte Einigkeit darüber, welche Profile und zugehörigen Kompetenzen die Arbeitskräfte im Cybersicherheitsbereich in der EU in ihrer Gesamtheit abdecken sollten, wobei für ähnliche Berufsprofile im Cybersicherheitsbereich dieselben Kompetenzen erforderlich sein sollten. Die geringe Akzeptanz eines gemeinsamen **europäischen Referenzrahmens für Cybersicherheitsfachkräfte** durch die relevanten

[17] Cybersecurity Higher Education Database (CyberHEAD).

[18] Nur 19 % der IKT-Fachkräfte in der EU sind Frauen (Digital Economy and Society Index (DESI) 2022 | Shaping Europe’s digital future (europa.eu)). Es liegen keine Zahlen zu den weiblichen Arbeitskräften im Cybersicherheitsbereich in der Union vor.

[19] Beschluss (EU) 2022/2481 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Aufstellung des Politikprogramms 2030 für die digitale Dekade, mit dem ein Überwachungs- und Kooperationsmechanismus eingerichtet wurde, damit die im digitalen Kompass 2030 festgelegten gemeinsamen Ziele und Vorgaben für den digitalen Wandel in Europa erreicht werden, auch im Bereich Kompetenzen.

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

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

[22] SME definition (europa.eu).

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

Akteure schlägt sich im Fehlen eines Instruments für die Kommunikation zwischen Arbeitgebern, Lehrkräften und politischen Entscheidungsträgern und in der Unmöglichkeit nieder, Messungen durchzuführen und die Lücken auf dem Cybersicherheitsarbeitsmarkt zu bewerten. Zudem verhindert dies die Entwicklung entsprechender Lehrpläne für die allgemeine und berufliche Bildung und die Schaffung von Laufbahnen, die dem strategischen Bedarf und der Marktnachfrage Rechnung tragen und auf diejenigen ausgerichtet sind, die einen Beruf in diesem Bereich ergreifen wollen. Die **Weiterbildung und Umschulung** der Arbeitskräfte beruht weitgehend auf Cybersicherheitsschulungen und -zertifikaten, die üblicherweise von privaten Anbietern angeboten werden. Es ist jedoch schwierig für die Arbeitskräfte, sich einen Überblick über die Qualität der angebotenen Cybersicherheitsschulungen und der zugehörigen ausgestellten Zertifikate zu verschaffen.

Allgemeine und berufliche Bildung sowie Laufbahnentwicklung sind notwendig für die Verbesserung des Angebots auf dem Arbeitsmarkt, doch die Rolle der **Nachfrageseite** im Bereich der beruflichen Bildung der Arbeitskräfte und der Anpassung an die Entwicklung des Arbeitsmarkts wird derzeit unterschätzt. Der Wirtschaft und öffentlichen Arbeitgebern mangelt es an gemeinsamen Foren und Orten dafür, Ideen für die bestmögliche Schulung der Arbeitskräfte zu bündeln und sich mit der **besseren Bewertung von Kompetenzen**, insbesondere während der Einstellungsverfahren, zu befassen. Die am stärksten gefragten **fachlichen Kompetenzen** mögen zwar cybersicherheitsbezogene Kompetenzen[24] wie solche im Bereich der Softwareentwicklung oder des Cloud-Computings[25] sein, doch **Querschnittskompetenzen** werden ungerechtfertigterweise nach wie vor außer Acht gelassen. Kritisches Denken und kritische Analysen, Problemlösung und Selbstmanagement sind Kompetenzgruppen, die von den Arbeitgebern verstärkt verlangt werden[26] und die bis 2025 an Bedeutung gewinnen[27].

Es gibt bereits viele Initiativen für öffentliche und private Investitionen in Cybersicherheitskompetenzen, und die EU **fördert** im Rahmen verschiedener Instrumente in großem Umfang Projekte[28]. Der anhaltende Mangel an Kompetenzen in der EU wirft allerdings Fragen hinsichtlich der Sichtbarkeit und Wirkung der Initiativen auf und deutet darauf hin, dass sie möglicherweise nicht systematisch dem Marktbedarf entsprechen, der dringend auf EU-Ebene erfasst werden muss. Darüber hinaus führt das Vorhandensein mehrerer Finanzierungsquellen zu Doppelungen, und die Gelegenheit, die Initiativen auszuweiten und eine echte Wirkung zu erzielen, wird verpasst. Zudem können diejenigen, die Investitionen benötigen, nicht immer die zur Deckung ihres Bedarfs am besten geeigneten Quellen ermitteln.

**Interessenträger** haben versucht, das komplexe und vielschichtige Problem des Mangels an Cybersicherheitskompetenzen anzugehen. Die Agentur der Europäischen Union für Cybersicherheit (ENISA) hat Instrumente zu Aufgabenprofilen bzw. zur Hochschulbildung entwickelt[29], das Europäische Kompetenzzentrum für Cybersicherheit[30] befasst sich in einer

[24] LinkedIn 2023 Most In-Demand Skills: Learn the skills companies need most.

[25] ISACA State of Cyber Security 2022 infographic.

[26] Z. B. Cedefop-Tool: Skills-OVATE | CEDEFOP (europa.eu).

[27] The Future of Jobs Report, Oktober 2020, Weltwirtschaftsforum.

[28] Z. B.: Cybersecurity Skills Alliance – A New Vision for Europe – Projekt REWIRE (im Rahmen des Programms Erasmus+ gefördert); Projekte zur Unterstützung des Kompetenzzentrums für Cybersicherheit (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (im Rahmen von Horizont 2020 gefördert), Projekt CyberSecPro (im Rahmen des Programms „Digitales Europa“ gefördert)).

[29] Insbesondere: Europäischer Kompetenzrahmen für Cybersicherheit (ECSF); Cybersecurity Higher Education Database (CyberHEAD); Cyberübungsplattform (Cyber Exercise Platform – CEP); European Cyber Security Challenge; europäischer Monat der Cybersicherheit.

einschlägigen Arbeitsgruppe mit Cybersicherheitskompetenzen, das Europäische Sicherheits- und Verteidigungskolleg (ESVK) beschäftigt sich mit Cybersicherheitskompetenzen zivilen und militärischen Personals im Kontext der Gemeinsamen Sicherheits- und Verteidigungspolitik[31], private Organisationen versuchen, das Problem in Angriff zu nehmen[32], und die Cybersicherheitszertifizierungsbranche arbeitet einen Fahrplan und Schulungen zur Schließung der Kompetenzlücke aus[33]. Die Mitgliedstaaten versuchen auch, das Problem mit einer Vielzahl von Initiativen – von regulatorischen Initiativen[34] bis hin zur Einrichtung von Akademien für Cybersicherheitskompetenzen[35], Cyber-Campus[36] oder Cyberkriminalität-Exzellenzzentren[37] – oder durch öffentlich-private Partnerschaften[38] anzugehen. Allerdings fehlt es bei der Arbeit all dieser Interessenträger häufig an Koordinierung und Synergieeffekten, und das Potenzial, auf dem Arbeitsmarkt eine spürbare Wirkung zu erzielen, wurde bislang nicht ausgeschöpft, was der zunehmende Mangel an Arbeitskräften im Cybersicherheitsbereich in der EU veranschaulicht. Zudem muss die Zahl der Synergieeffekte zwischen Cybergemeinschaften erhöht werden, da die nötigen Kompetenzen für die Aufrechterhaltung der Cybersicherheit, die Bekämpfung der **Cyberkriminalität** oder die Entwicklung von **Cyberabwehrreaktionen** oft ähnlich sind.

Der EU stehen derzeit begrenzte Mittel zur Bewertung des **Zustands und der Entwicklung des Cybersicherheitsarbeitsmarkts** und der Kompetenzen der Arbeitskräfte in diesem Bereich zur Verfügung. Die Mitgliedstaaten und die Organe, Einrichtungen und sonstigen Stellen der Europäischen Union stützen sich auf von privaten Einrichtungen erhobene Daten oder auf einen breiteren Satz von Daten zu IKT-Fachkräften, die insbesondere von Eurostat[39] und dem Europäischen Zentrum für die Förderung der Berufsbildung (Cedefop)[40] in der EU erhoben werden. Somit hat die EU nur einen partiellen und fragmentierten Einblick in ihren Bedarf, was sie daran hindert, sich einen gebündelten Überblick über die Lage auf dem Cybersicherheitsarbeitsmarkt zu verschaffen.

## 3. Eine EU-weite abgestimmte Reaktion: die Akademie für Cybersicherheitskompetenzen

### *3.1.Ziel*

Wie die Präsidentin der Europäischen Kommission in ihrer Absichtserklärung zur Lage der Union 2022[41, 42] und im Zusammenhang mit dem Europäischen Jahr der Kompetenzen

---

[30] Verordnung (EU) 2021/887 des Europäischen Parlaments und des Rates vom 20. Mai 2021 zur Einrichtung des Europäischen Kompetenzzentrums für Industrie, Technologie und Forschung im Bereich der Cybersicherheit und des Netzwerks nationaler Koordinierungszentren.

[31] Insbesondere: Plattform zur Aus- und Fortbildung, Evaluierung und Übung im Cyberbereich (ETEE).

[32] Z. B.: Arbeitsgruppe 5 der Europäischen Cybersicherheitsorganisation (ECSO) zum Thema „Allgemeine und berufliche Bildung, Sensibilisierung, Cyber-Ranges und menschliche Faktoren“; Organisation DIGITALEUROPE.

[33] Z. B.: SANS-Institut, (ISC)² und ISACA.

[34] Z. B. mit nationalen Strategien für Bildung oder Cybersicherheit.

[35] Z. B.: C-Academy in Portugal.

[36] Z. B.: mehrere Cyber-Campus in Frankreich.

[37] Z. B.: litauisches Cyberkriminalität-Exzellenzzentrum für berufliche Bildung, Forschung und allgemeine Bildung in Litauen (L3CE).

[38] Z. B.: Microsofts Initiative zur Vermittlung von Cybersicherheitskompetenzen.

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

[40] Z. B. Cedefop-Tool: Skills-OVATE | CEDEFOP (europa.eu).

[41] Absichtserklärung zur Lage der Union 2022 an Präsidentin Roberta Metsola und Ministerpräsident Petr Fiala.

[42] Gemeinsame Mitteilung an das Europäische Parlament und den Rat, EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

angekündigt hat, schlägt die Kommission eine **Akademie für Cybersicherheitskompetenzen** vor, um die Herausforderung, die Cybersicherheitskompetenzen auszubauen und die Lücke auf dem Arbeitsmarkt zu schließen, zu bewältigen.

Mit der Akademie für Cybersicherheitskompetenzen (Kurzform: „Akademie“) sollen eine **zentrale Anlaufstelle und Synergieeffekte** in Bezug auf das Angebot im Bereich der allgemeinen und beruflichen Cybersicherheitsbildung geschaffen sowie Finanzierungsmöglichkeiten und spezifische Maßnahmen zur Unterstützung der Entwicklung von Cybersicherheitskompetenzen eingeführt werden. Die Akademie wird Initiativen von Interessenträgern so verstärken, dass eine „kritische Masse“ erreicht und eine spürbare Wirkung auf dem Arbeitsmarkt erzielt wird, auch in Bezug auf die Abwehr. Die entsprechenden Tätigkeiten würden an gemeinsamen Zielen und wesentlichen Leistungsindikatoren ausgerichtet, damit eine größere Wirkung erzielt wird.

Die Akademie wird sich auf die Vermittlung von Kompetenzen für **Cybersicherheitsfachkräfte** konzentrieren. Die Tätigkeit der Akademie wird in die EU-Cybersicherheitspolitik, aber auch in den Bereich Bildung und lebenslanges Lernen einfließen. Sie ergänzt die beiden von der Kommission zeitgleich mit der vorliegenden Mitteilung vorgeschlagenen Empfehlungen des Rates zu digitaler Bildung und digitalen Kompetenzen[43].

Die Akademie wird sich auf vier Säulen stützen: 1) Förderung der **Wissensgenerierung im Rahmen der allgemeinen und beruflichen Bildung** dadurch, dass ein gemeinsamer Rahmen für Cybersicherheitsaufgabenprofile und zugehörige Kompetenzen aufgestellt wird, das Angebot im Bereich der allgemeinen und beruflichen Bildung in Europa verbessert wird, um den Bedarf zu decken, Laufbahnen entwickelt werden und Cybersicherheitsschulungen und -zertifizierungen sichtbar gemacht werden und in diesem Bereich mehr Klarheit geschaffen wird, um das Angebot auf dem Arbeitsmarkt zu verbessern; 2) gezielterer Einsatz von Mitteln und Verbesserung der Sichtbarkeit der verfügbaren **Finanzierungsmöglichkeiten** für kompetenzbezogene Tätigkeiten zur Maximierung ihrer Wirkung; 3) Aufruf an die Interessenträger, **tätig zu werden**; 4) Festlegung von Indikatoren, um die **Marktentwicklung zu überwachen** und die Wirksamkeit der Maßnahmen bewerten zu können.

Die Einrichtung der Akademie wird mit 10 Mio. EUR aus dem Programm „Digitales Europa“[44] unterstützt.

### *3.2. Verwaltung der Akademie*

Die Akademie könnte letztendlich die Form eines **Konsortiums für europäische Digitalinfrastrukturen (EDIC)**[45] annehmen, damit eine Infrastruktur geschaffen wird, die als **zentrale Anlaufstelle** dient, die die Zusammenarbeit zwischen Wissenschaft, Schulungsanbietern und Wirtschaft fördert und bei der Angebot und Nachfrage des EU-Cybersicherheitsökosystems aufeinandertreffen und Schulungen durchgeführt werden können. Ein derartiges Instrument würde es den Mitgliedstaaten ermöglichen, gemeinsam an

[43] Vorschlag für eine Empfehlung des Rates zu den Schlüsselfaktoren für eine erfolgreiche allgemeine und berufliche digitale Bildung und Vorschlag für eine Empfehlung des Rates für eine bessere Vermittlung digitaler Kompetenzen in der allgemeinen und beruflichen Bildung.

[44] Verordnung (EU) 2021/694 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Aufstellung des Programms „Digitales Europa“ und zur Aufhebung des Beschlusses (EU) 2015/2240.

[45] Die EDIC wurden mit Artikel 13 ff. des Beschlusses (EU) 2022/2481 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Aufstellung des Politikprogramms 2030 für die digitale Dekade eingeführt.

der Schließung der Lücke bei Cybersicherheitskompetenzen zu arbeiten sowie – im Einklang mit deren jeweiligen Mandaten und Befugnissen – eng mit der Kommission, der ENISA und dem Europäischen Kompetenzzentrum für Cybersicherheit zusammenzuarbeiten und alle einschlägigen Interessenträger zur Beteiligung zu bewegen. Zudem könnte man dadurch europäische, nationale und private Investitionen auf ein gemeinsames Ziel ausrichten. Zu diesem Zweck werden interessierte Mitgliedstaaten aufgefordert, die Kommission bis zum 30. Mai 2023 vorab über einen künftigen Antrag für ein derartiges EDIC zu informieren. Dank einer derartigen freiwilligen Vorabinformation könnte die Kommission frühzeitig zum Entwurf des EDIC-Antrags Stellung nehmen, was eine schnellere Weiterentwicklung und förmliche Einreichung ermöglichen würde. Die Kommission wird als Beschleuniger für Mehrländerprojekte die Vorbereitung des EDIC-Antrags während des gesamten Verfahrens in dem von den jeweiligen Mitgliedstaaten gewünschten Ausmaß erleichtern. Daraufhin erlässt die Kommission, nachdem sie den Antrag positiv bewertet und der Ausschuss für das Programm für die digitale Dekade ihn genehmigt hat, einen Beschluss zur Einrichtung des EDIC und hilft danach bei der Koordinierung der Umsetzung des EDIC[46].

In der Zwischenzeit – während der förmlichen Einrichtung des EDIC – schafft die Kommission eine virtuelle zentrale Anlaufstelle, indem sie die **Plattform der Kommission für digitale Kompetenzen und Arbeitsplätze**[47] mit Unterstützung des Projekts zur Unterstützung der europäischen Cybersicherheitsgemeinschaft (ECCO)[48] ausbaut.

Die **ENISA** wird im Einklang mit ihren Zielen[49] unter Berücksichtigung ihrer Berichtspflichten gemäß der NIS-2-Richtlinie[50] zur Einrichtung der Akademie beitragen, insbesondere im Hinblick auf die Unterstützung bei der allgemeinen und beruflichen Cybersicherheitsbildung. Das **Europäische Kompetenzzentrum für Cybersicherheit** wird im Einklang mit seiner strategischen Agenda daran arbeiten, die Einrichtung der Akademie für Cybersicherheitskompetenzen zu unterstützen. Das Kompetenzzentrum wird insbesondere das dritte strategische Ziel (Cybersicherheit) des Programms „Digitales Europa“ umsetzen. Es wird von der Kommission sowie über die **nationalen Koordinierungszentren** von den Mitgliedstaaten unterstützt. Erforderlichenfalls wird die mit der NIS-2-Richtlinie[51] eingesetzte **Kooperationsgruppe** hinzugezogen. Zudem muss mit der **Wirtschaft** und der **Wissenschaft** zusammengearbeitet werden, um die Lücke bei Cybersicherheitskompetenzen – wie von der Akademie angestrebt – zu schließen.

### 4. Wissensgenerierung und berufliche Bildung: Festlegung eines gemeinsamen EU-Ansatzes für berufliche Cybersicherheitsbildung

---

[46] Ebenda, Artikel 12.

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

[48] Siehe: European Cybersecurity Competence Centre and Network: new EU-funded project to support the Cyber Community (europa.eu). Die Europäische Kommission vergab im Dezember 2022 einen Auftrag im Wert von 3 Mio. EUR zur Unterstützung der EU-Cybergemeinschaft im Rahmen des Europäischen Kompetenzzentrums für Cybersicherheit. Das entsprechende Projekt wird zur Verwirklichung der Ziele der EU im Bereich Aufbau von Gemeinschaften und Kapazitäten in Bezug auf Forschung, Innovationen, Akzeptanz und die industrielle Basis im Cybersicherheitsbereich beitragen.

[49] „Die ENISA fördert unionsweit den Kapazitätsaufbau und die Abwehrbereitschaft, indem sie die Organe, Einrichtungen und sonstigen Stellen der Union, die Mitgliedstaaten sowie öffentliche und private Interessenträger dabei unterstützt, … Fähigkeiten und Kompetenzen auf dem Gebiet der Cybersicherheit aufzubauen.“ Artikel 4 Absatz 3 des Rechtsakts zur Cybersicherheit.

[50] Artikel 18 der NIS-2-Richtlinie.

[51] Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie).

Im Rahmen der Säule der Akademie für Cybersicherheitskompetenzen für Wissensgenerierung und berufliche Bildung wird ein strukturierter Ansatz entwickelt; dabei wird das klare Ziel verfolgt, die **Zahl** der Menschen mit Cybersicherheitskompetenzen in der EU zu erhöhen, Schulungen besser an den **Bedarf auf dem Markt** anzupassen und **Laufbahnen** sichtbar zu machen.

### *4.1. Dieselbe Sprache sprechen: ein gemeinsamer Ansatz für Cybersicherheitsaufgabenprofile und zugehörige Kompetenzen*

Die ENISA hat im Rahmen des Europäischen Kompetenzrahmens für Cybersicherheit (**ECSF**)[52] bereits an der Festlegung von Aufgabenprofilen für Cybersicherheitsfachkräfte gearbeitet. Auf dieser Grundlage sollte die Akademie relevante Kompetenzen festlegen und bewerten, die Entwicklung der Kompetenzlücken überwachen und Angaben zum neuen Bedarf machen. Für jede Cybersicherheitsaufgabe des ECSF wird eine Reihe einschlägiger Kompetenzen aus dem europäischen Rahmen für IKT-Kompetenzen (e-CF)[53] als Element in die Profilbeschreibung aufgenommen[54].

Die ENISA wird daher den ECSF überprüfen und **sich abzeichnende Kompetenzbedürfnisse und -lücken** bei den Arbeitskräften im Cybersicherheitsbereich **ermitteln**, unter anderem mit fortschrittlichen Hilfsmitteln (z. B. künstliche Intelligenz, Big Data[55], Data Mining). Zu diesem Zweck wird die ENISA unter der Leitung des EDIC – sobald es eingerichtet wurde – und des Europäischen Kompetenzzentrums für Cybersicherheit mit nationalen Koordinierungszentren, der Kommission, dem ECCO-Projekt und Marktteilnehmern zusammenarbeiten.[56] Im Hinblick auf die Arbeitskräfte im Bereich der Cyberabwehr wird die ENISA die Arbeit des ESVK gebührend berücksichtigen. Zudem wird die ENISA im Bereich der Bekämpfung der Cyberkriminalität den Tätigkeiten der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) und von Europol Rechnung tragen, wenn sie eine Analyse des Bedarfs an operativen Schulungen[57] zu Cyberangriffen einführt.

Der ECSF wird im Rahmen der Akademie während eines Zweijahreszyklus regelmäßig ergänzt und überprüft. Darüber hinaus werden die Kommission und der Europäische Auswärtige Dienst nach Bedarf zur Festlegung spezifischer Profile und der zugehörigen Kompetenzen für bestimmte Bereiche beitragen, und zwar mit Unterstützung von Einrichtungen und sonstigen Stellen der EU wie dem ESVK[58], Europol und CEPOL[59].

---

[52] European Cybersecurity Skills Framework (ECSF) — ENISA (europa.eu). Mit dem ECSF wird die Ermittlung und Formulierung von Aufgaben, Fähigkeiten, Kompetenzen und Kenntnissen im Zusammenhang mit den Aufgaben europäischer Cybersicherheitsfachkräfte unterstützt. Er fasst alle Aufgaben im Zusammenhang mit der Cybersicherheit in Profilen zusammen, die individuell mit Blick auf die Einzelheiten der entsprechenden Zuständigkeiten, Kompetenzen, Synergieeffekte und gegenseitigen Abhängigkeiten analysiert werden.

[53] European e-Competence Framework (e-CF) | Esco (europa.eu). Der e-CF schafft schlüssige Verbindungen im Zusammenhang mit IKT-Qualifikationen und anderen für den Bereich relevanten Rahmen, darunter DigComp.

[54] Siehe hierzu: User Manual – European Cybersecurity Skills Framework (ECSF) – September 2022.

[55] Siehe z. B.: Skills-OVATE, entwickelt vom Cedefop.

[56] Die Agentur wird die Ergebnisse anderer von der EU finanzierter Projekte (z. B. REWIRE, Data Space For Skills (DS4S), CyberSecPro, CONCORDIA) und Methoden nutzen, die von ähnlichen Initiativen (z. B. OECD-Bericht mit dem Titel „Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States“ vom 21. März 2023) abgeleitet sind, um dafür zu sorgen, dass in Zukunft ein aktueller Überblick über den Bedarf in einem Umfeld mit sich ständig ändernder Nachfrage besteht.

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

[58] Siehe hierzu: Gemeinsame Mitteilung an das Europäische Parlament und den Rat, EU-Cyberabwehrpolitik, JOIN(2022) 49 final.

Ferner werden Verbindungen zwischen dem ECSF und relevanten Instrumenten der EU-Beschäftigungspolitik[60] hergestellt. Insbesondere die ECSF-Berufsprofile und die zugehörigen Kompetenzen werden in die **ESCO-Klassifikation** integriert. Dadurch werden die Klassifikation von Berufen und Kompetenzen im Cybersicherheitsbereich und deren Verknüpfungen verbessert, was es Einzelpersonen erleichtert, sich weiterzubilden und umzuschulen, und wodurch der kompetenzbasierte Abgleich von Stellenangeboten mit Stellengesuchen und die grenzüberschreitende Mobilität unterstützt werden.

### *4.2. Förderung der Zusammenarbeit bei der Gestaltung von Lehrplänen für die allgemeine und berufliche Cybersicherheitsbildung*

Sobald das EDIC eingerichtet wurde, sollte die Akademie von den Mitgliedstaaten unterstützt werden, damit sie zur **europäischen Referenzstelle für die Gestaltung und Durchführung von Cybersicherheitsschulungen** zu den am stärksten gefragten Kompetenzen wird und Schulungen am Arbeitsplatz und Praktikumsmöglichkeiten für Start-up-Unternehmen und KMU sowie für öffentliche Verwaltungen in innovativen Unternehmen im Cybersicherheitsbereich und in Cybersicherheitskompetenzzentren anbieten kann. Das EDIC sollte mit allen einschlägigen Interessenträgern, einschließlich solchen aus der Wirtschaft, zusammenarbeiten, um derartige Schulungen zu gestalten, und dabei auf Projekten wie **CyberSecPro**[61] aufbauen, das im Rahmen des Programms „Digitales Europa“ finanziert wird und 17 Hochschuleinrichtungen und 13 Sicherheitsunternehmen aus 16 Mitgliedstaaten zusammenbringt, um bewährte Verfahren für Cybersicherheitsschulungsprogramme jeglicher Art zu etablieren.

Die Akademie wird mit allen einschlägigen Interessenträgern zusammenarbeiten, um Laufbahnen im Cybersicherheitsbereich **für die jungen Generationen attraktiv zu machen**. Die Mitgliedstaaten sollten im Einklang mit dem Vorschlag für eine Empfehlung des Rates für eine bessere Vermittlung digitaler Kompetenzen in der allgemeinen und beruflichen Bildung Maßnahmen für die Gewinnung und Schulung von Fachlehrkräften und Ausbildenden einführen und verstärken und den Erwerb von Cybersicherheitskompetenzen unter anderem durch Ausbildungsplätze erleichtern. Folgendes sollte gefördert werden: die Einbeziehung der Cybersicherheit in Programme für allgemeine und berufliche Bildung unter Sicherstellung ihrer Zugänglichkeit, die Entwicklung von **Ausbildungs-** und Praktikumsangeboten, die Förderung innovativer Ansätze, darunter z. B. digitale Lernspiele und gemeinsame Plattformen für Simulationen, die Organisation von Immersionswochen für Arbeitsstellen im Cybersicherheitsbereich und die Erläuterung der nichttechnischen Aufgabenprofile. Zudem sollte die Wahrnehmung derartiger Lernmöglichkeiten durch schwer zu erreichende Gruppen wie junge Menschen, die Behinderungen haben, in abgelegenen oder ländlichen Gebieten wohnen oder anderen Minderheitengruppen angehören, unterstützt werden.

---

[59] In diesem Zusammenhang wird der Arbeit an dem Kompetenzrahmen für Cyberkriminalitätsschulungen (TCF), der derzeit entwickelt wird, Rechnung getragen.

[60] Z. B.: europäische Klassifizierung für Fähigkeiten/Kompetenzen, Qualifikationen und Berufe (ESCO), Europass und Europäisches Netz der Arbeitsvermittlungen (EURES).

[61] CyberSecPro. Es werden beispielsweise die an den Hochschulen angebotenen Programme und (Sommer-)Kurse im Cybersicherheitsbereich und die herangezogenen Einstufungstabellen des Europäischen Systems zur Übertragung und Akkumulierung von Studienleistungen (ECTS) analysiert; zudem wird dafür gesorgt, dass innerhalb von drei Jahren über 530 Praktika absolviert werden können, und es werden Externe aus verschiedenen Branchen und Bereichen geschult.

Die Kommission wird die Entwicklung von Microcredentials und Programmen für berufliche Aus- und Weiterbildung weiterhin unterstützen. Insbesondere werden im Rahmen von Erasmus+ auch künftig **gemeinsame Bachelor- und Masterstudiengänge, gemeinsame Kurse oder Module, bei denen Microcredentials erworben werden können**, und **gemischte Intensivprogramme**[62] zu allen Themen finanziert, unter anderem **zur Cybersicherheit**. Zudem werden die weitere Umsetzung der **Initiative „Europäische Hochschulen“**[63] und die weitere Einführung von **Zentren der beruflichen Exzellenz**[64] unterstützt, um eine verstärkte Zusammenarbeit zwischen Hochschuleinrichtungen und einschlägigen Einrichtungen für berufliche Bildung in ganz Europa zu fördern. Die Verwirklichung des Ziels der vertieften Zusammenarbeit wird durch EU-Finanzierungsprogramme, unter anderem durch Erasmus+ und das Programm „Digitales Europa“, sowie durch EU-Mittel für die Entwicklung **individueller Lernkonten**[65] unterstützt.

Die nationalen Koordinierungszentren werden aufgefordert, die Möglichkeit, **Cyber-Campus** in den Mitgliedstaaten einzurichten, zu prüfen, um die Zusammenarbeit zwischen Wissenschaft und Anbietern von Schulungen zu Cybersicherheitskompetenzen mit Arbeitgebern aus dem privaten und dem öffentlichen Sektor auf nationaler Ebene zu erleichtern und Synergieeffekte zwischen dem öffentlichen und dem privaten Sektor zu fördern. Mit den Cyber-Campus würde angestrebt, auf nationaler Ebene Exzellenzzentren für die Cybersicherheitsgemeinschaft bereitzustellen, und die Akademie würde die Vernetzung der Campus und die weitere Abstimmung ihrer Tätigkeiten unterstützen.

Die ENISA wird außerdem ihr Schulungsangebot im Cybersicherheitsbereich erweitern, **ihren Kurskatalog**[66] an die ECSF-Profile anpassen und Schulungsmodule für jedes Profil entwickeln, wodurch möglicherweise das Schulungsangebot der Mitgliedstaaten erweitert wird. Zudem wird die ENISA ihr **Programm zur Ausbildung Ausbildender**[67] erweitern und dabei den beruflichen Bedürfnissen der Organe, Einrichtungen und sonstigen Stellen der Europäischen Union sowie der Behörden der Mitgliedstaaten und **öffentlicher und privater kritischer Betreiber** im Rahmen der NIS-2-Richtlinie Rechnung tragen.

Darüber hinaus werden andere Einrichtungen und sonstige Stellen der EU ihr Schulungsangebot im Cybersicherheitsbereich verstärken. So wird das **ESVK** beispielsweise zur Umsetzung der EU-Cyberabwehrpolitik eine neue Reihe von Cybersicherheitskursen entwickeln und einige seiner aktuellen Kurse an den ECSF anpassen. Diese Kurse werden zur Zertifizierung von Lernergebnissen[68] führen. Das ESVK wird in Zusammenarbeit mit der Kommission die Möglichkeit der Aufnahme von Zertifikaten in die EUid-Brieftasche prüfen. Das ESVK wird ferner die mögliche Bewertung von Kompetenzmechanismen zur Ausstellung von Zertifikaten prüfen. Zudem werden im Bereich der Bekämpfung der Cyberkriminalität enge Beziehungen zur **CEPOL-Akademie zur Bekämpfung der**

[62] Bei gemischten Intensivprogrammen wird Online-Unterricht mit einem kurzen Mobilitätsaufenthalt kombiniert.

[63] Initiative „Europäische Hochschulen“ | European Education Area (europa.eu).

[64] Zentren der beruflichen Exzellenz | Erasmus+ (europa.eu).

[65] Im Einklang mit der Empfehlung des Rates vom 16. Juni 2022 zu individuellen Lernkonten.

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

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

[68] Im Einklang mit Artikel 20 Absatz 4 des Beschlusses (GASP) 2020/1515 des Rates vom 19. Oktober 2020 zur Errichtung eines Europäischen Sicherheits- und Verteidigungskollegs und zur Aufhebung des Beschlusses (GASP) 2016/2382.

**Cyberkriminalität**[69] angestrebt, um Synergieeffekte und Komplementaritäten bei der Gestaltung und Umsetzung von Lehrplänen für die berufliche Bildung zu fördern.

### *4.3.Schaffung von Synergieeffekten und bessere Sichtbarkeit von Cybersicherheitsschulungen und -zertifizierungen in allen Mitgliedstaaten*

Die Akademie sollte sich mit der Sichtbarkeit von Schulungen und Zertifizierungen und einschlägigen Synergieeffekten befassen. Dies käme den Cybergemeinschaften in der Zivilgesellschaft, im Verteidigungswesen, in der Strafverfolgung und in der Diplomatie zugute, da dort in vielen Fällen dasselbe Fachwissen auf der Grundlage ähnlicher Lehrpläne und Lernergebnisse benötigt wird.

Die Akademie würde als **zentrale Anlaufstelle** für Menschen dienen, die sich für eine Laufbahn im Cybersicherheitsbereich interessieren. Dies wird kurzfristig erreicht, indem die **Plattform der Kommission für digitale Kompetenzen und Arbeitsplätze** mit Unterstützung des ECCO-Projekts erweitert wird. In einem speziellen Bereich für Laufbahnen im Cybersicherheitsbereich werden bestehende Hilfsmittel wie Hochschulprogramme oder Schulungsmöglichkeiten – darunter Kurse, bei denen Microcredentials erworben werden können, und Programme für berufliche Bildung – mit Stellenangeboten verknüpft. Dafür werden laufende Maßnahmen und Initiativen auf der Plattform genannt oder in sie integriert, z. B. Aktivitäten der ENISA, die in Zusammenarbeit mit der Wissenschaft **Bildungseinrichtungen erfasst**, die Cybersicherheitsprogramme anbieten. In diesem Bereich werden mit Unterstützung der nationalen Koordinierungszentren weitere Verbesserungen vorgenommen. Außerdem wird die ENISA mit Unterstützung der nationalen Koordinierungszentren, der Kommission und des ECCO-Projekts und in Zusammenarbeit mit Zertifikaten vergebenden Einrichtungen zwei **Repositorys für bestehende Schulungen aus dem öffentlichen und dem privaten Sektor und für Cybersicherheitszertifizierungen** entwickeln und konsolidieren, wobei auch auf anderen einschlägigen Initiativen[70] aufgebaut wird. Diese werden auch in die zentrale Anlaufstelle der Plattform für digitale Kompetenzen und Arbeitsplätze integriert. Diese Arbeit wird auch den nationalen Koordinierungszentren zugutekommen, die insbesondere dafür zuständig sind, Bildungsprogramme im Cybersicherheitsbereich zu fördern und zu verbreiten[71].

Außerdem müssen Fachkräfte darauf vertrauen können, dass ihre Schulungen die erforderliche Qualität haben. Dazu wird die ENISA ein **Pilotprojekt** entwickeln, in dem die Möglichkeit der Einrichtung eines europäischen Zertifizierungssystems für Cybersicherheitskompetenzen geprüft wird.

Zudem sind die Ermittlung von Kompetenzen und Schulungen und ihre Verknüpfung mit einem Berufsprofil von wesentlicher Bedeutung, doch es ist auch wichtig, dass dafür gesorgt wird, dass Anbieter von Cybersicherheitsdiensten über das notwendige Maß an Kompetenz, Fachwissen und Erfahrung verfügen. Dies gilt insbesondere für Anbieter verwalteter

---

[69] Die CEPOL-Akademie zur Bekämpfung der Cyberkriminalität wurde 2019 eingerichtet, um eine hochmoderne Plattform zur Verbesserung des Wissens über Cyberkriminalität und der Cyberkapazitäten in Europa bereitzustellen.

[70] Z. B.: W4C Academy – Women4Cyber oder Global Cybercrime Certification project für Strafverfolgungs- und Justizbehörden.

[71] „(1) Die nationalen Koordinierungszentren haben folgende Aufgaben: … g) sie arbeiten mit den Behörden der Mitgliedstaaten im Hinblick auf einen möglichen Beitrag zur Förderung und Verbreitung von Schulungsprogrammen im Bereich Cybersicherheit zusammen, unbeschadet der Zuständigkeiten der Mitgliedstaaten für Bildung und unter Berücksichtigung der einschlägigen Aufgaben der ENISA;“ (Artikel 7 Absatz 1 Buchstabe g der Verordnung zur Einrichtung des Europäischen Kompetenzzentrums für Cybersicherheit). Siehe auch den einschlägigen Erwägungsgrund 28.

Sicherheitsdienste in Bereichen wie Reaktion auf Sicherheitsvorfälle, Penetrationstests, Sicherheitsaudits und Beratung. In der NIS-2-Richtlinie und dem Vorschlag für den Rechtsakt zur Cybersolidarität werden spezifische Aufgaben für derartige Anbieter verwalteter Sicherheitsdienste festgelegt. Daher schlägt die Kommission auch eine **gezielte Änderung des Rechtsakts zur Cybersicherheit**[72] vor, um Zertifizierungsschemata für verwaltete Sicherheitsdienste auf EU-Ebene zu ermöglichen. Solche Zertifizierungsschemata sollten unter anderem darauf abzielen, dass die Dienste von Personal mit sehr großem Fachwissen und sehr hoher Kompetenz in den relevanten Bereichen angeboten werden.

**Qualitätssicherungs- und Anerkennungsmechanismen für Microcredentials**[73] sind der Transparenz, Vergleichbarkeit und Übertragbarkeit von Lernergebnissen zuträglich. Im Einklang mit der Empfehlung des Rates über einen europäischen Ansatz für Microcredentials[74] werden die Mitgliedstaaten aufgefordert, Microcredentials für Cybersicherheit in ihre nationalen Qualifikationsrahmen aufzunehmen. Dies würde es ihnen ermöglichen, Microcredentials für Cybersicherheit mit dem Europäischen Qualifikationsrahmen[75] zu verknüpfen. Die Infrastruktur für europäische digitale Zertifikate steht für die Ausstellung digital unterzeichneter Qualifikationsnachweise und Microcredentials von Einzelpersonen im Cybersicherheitsbereich zur Verfügung. Diese umfassen umfangreiche Daten, unter anderem Daten zu Lernergebnissen im Cybersicherheitsbereich, und können in der künftigen **digitalen EUid-Brieftasche**[76] gespeichert werden.

**Maßnahmen im Rahmen der Akademie**

**Mitgliedstaaten und Wirtschaft**

- Unterstützung der Entwicklung und Anerkennung von **Microcredentials** für das Lernen im Cybersicherheitsbereich im Einklang mit der Empfehlung des Rates über einen europäischen Ansatz für Microcredentials.
- Aufnahme von Cybersicherheitsqualifikationsnachweisen, einschließlich Microcredentials, in **nationale Qualifikationsrahmen**.
- Anbieten von **Lernmöglichkeiten am Arbeitsplatz** im Rahmen von Ausbildungen für Menschen, die an Initiativen zur Entwicklung von Cybersicherheitskompetenzen teilnehmen.

**Kommission**

- Kurzfristig: Einrichtung einer **zentralen Anlaufstelle** für Cybersicherheitsprogramme, bestehende Schulungen und Cybersicherheitszertifizierungen über die **Plattform für digitale Kompetenzen und Arbeitsplätze** bis Ende 2023.

[72] Verordnung (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. April 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der Verordnung (EU) Nr. 526/2013 (Rechtsakt zur Cybersicherheit).

[73] Z. B.: Aufzeichnungen oder Zertifikate über die im Rahmen kurzer Schulungen erzielten Lernergebnisse.

[74] Empfehlung des Rates über einen europäischen Ansatz für Microcredentials für lebenslanges Lernen und Beschäftigungsfähigkeit.

[75] Empfehlung des Rates vom 22. Mai 2017 über den Europäischen Qualifikationsrahmen für lebenslanges Lernen und zur Aufhebung der Empfehlung des Europäischen Parlaments und des Rates vom 23. April 2008 zur Einrichtung des Europäischen Qualifikationsrahmens für lebenslanges Lernen.

[76] Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zur Änderung der Verordnung (EU) Nr. 910/2014 im Hinblick auf die Schaffung eines Rahmens für eine europäische digitale Identität.

- Vorschlagen einer Änderung des **Rechtsakts zur Cybersicherheit** am 18. April 2023, um eine Zertifizierung für Anbieter verwalteter Sicherheitsdienste zu ermöglichen.

**Einrichtungen und sonstige Stellen der EU**

- Etablierung des **ECSF** als gemeinsamen Ansatz für Cybersicherheitsaufgabenprofile und zugehörige Kompetenzen bis Ende 2023.
- Initiierung der Entwicklung eines Pilotprojekts zur Einrichtung eines **europäischen Zertifizierungssystems** für Cybersicherheitskompetenzen durch die ENISA im zweiten Quartal 2023.
- Überprüfung des **Kurskatalogs** der ENISA und Öffnung ihres **Programms zur Ausbildung Ausbildender** für öffentliche und private kritische Betreiber bis Ende 2023.
- **Anpassung der Lehrpläne des ESVK an den ECSF** bis Mitte 2023.

## 5. Einbeziehung der Interessenträger: Zusagen zur Schließung der Lücke bei Cybersicherheitskompetenzen

Im Rahmen der Akademie wird ein koordinierter Ansatz zur Einbeziehung der Interessenträger ausgearbeitet, um die Lücke bei Cybersicherheitskompetenzen zu schließen. Ziel ist es, die Sichtbarkeit und Wirkung der Zusagen der verschiedenen Interessenträger zur Verringerung der Lücke bei Cybersicherheitskompetenzen zu maximieren.

Die Kommission fordert die Interessenträger auf, konkrete Zusagen zu machen, indem sie sich zur Weiterbildung und Umschulung von Arbeitskräften durch entsprechende Maßnahmen verpflichten, und der ermittelten Lücke bei Cybersicherheitskompetenzen dabei in möglichst großem Umfang Rechnung zu tragen. Derartige **Cybersicherheitszusagen von Interessenträgern** sollten ähnlich wie andere bereits auf der Plattform angezeigte digitale Zusagen auf der **Plattform für digitale Kompetenzen und Arbeitsplätze** gemeldet werden. Die Kommission fordert die Interessenträger, die auf der Plattform Cybersicherheitszusagen machen, ferner dazu auf, sich der **groß angelegten Digitalpartnerschaft im Rahmen des Kompetenzpakts**[77] anzuschließen. Es wird begrüßt, wenn im Rahmen der groß angelegten Digitalpartnerschaft eingegangene Cybersicherheitsverpflichtungen auf der Plattform für digitale Kompetenzen und Arbeitsplätze eingereicht werden. Es wird ebenso begrüßt, wenn im Rahmen der Plattform für digitale Kompetenzen und Arbeitsplätze eingegangene Verpflichtungen im Zuge der groß angelegten Digitalpartnerschaft im Rahmen des Kompetenzpakts gemeldet werden.

Die Kommission fordert die Mitgliedstaaten ferner auf, **die Umsetzung der Erklärung zu Frauen im Digitalbereich**[78] **voranzutreiben**, um Frauen darin zu bestärken, eine aktive und wichtige Rolle im Bereich der Digitaltechnologie zu spielen, und um ein ausgewogeneres Geschlechterverhältnis in Cybersicherheitsberufen zu erreichen. Die Kommission fordert die Mitgliedstaaten zudem auf, Synergieeffekte mit ihren im Rahmen des **Europäischen Sozialfonds Plus** (ESF+) durchgeführten Programmen zu entwickeln, um weiter zur

[77] New European Partnerships launched to deliver on the EU's ambitions for the Digital Decade | Shaping Europe's digital future (europa.eu); die Partnerschaft wurde im Rahmen des Kompetenzpakts etabliert, um gegen die Defizite im IKT-Bereich vorzugehen.

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

Verwirklichung des Ziels der Geschlechtergleichstellung bei der Erwerbsbeteiligung[79] beizutragen, beispielsweise durch die Einrichtung von **Mentoringprogrammen für Frauen und Mädchen**. Diese können die Entstehung von Vorbildern begünstigen, die Cybersicherheitsberufe für Mädchen attraktiv machen, und zugleich zur Bekämpfung geschlechtsspezifischer Stereotype beitragen. Zudem werden die Weiterbildung und Umschulung von Frauen sowie die Entwicklung einer Gemeinschaft gefördert, was Frauen bei ihrem Eintritt in den Cybersicherheitsarbeitsmarkt und beim beruflichen Aufstieg in diesem Bereich unterstützen kann.

Die Mitgliedstaaten sollten **im Rahmen ihrer nationalen Cybersicherheitsstrategien spezifische Maßnahmen annehmen, um dem Mangel an Cybersicherheitskompetenzen entgegenzuwirken**[80], Maßnahmen zur Schließung der Kompetenzlücken zu ermitteln und diese gezielter einzusetzen und letztendlich die korrekte Erfüllung ihrer Verpflichtungen gemäß der NIS-2-Richtlinie sicherzustellen.

Einige Mitgliedstaaten nutzen **Synergieeffekte zwischen Initiativen im zivilen Bereich, in der Verteidigung und in der Strafverfolgung**. Beispielsweise könnten Cybersicherheits- und Cyberabwehrkompetenzen innerhalb der Bevölkerung, insbesondere bei jungen Erwachsenen, verbessert werden, wenn über den nationalen Pflichtwehrdienst ein größerer Personalbestand geschaffen würde oder Cyberreservistinnen und -reservisten – also in den Streitkräften im Cybersicherheitsbereich arbeitende Bürgerinnen und Bürger mit Militärausbildung – eingesetzt würden[81]. Dies gilt auch für die **Bekämpfung der Cyberkriminalität**, denn es bestehen viele Ähnlichkeiten zwischen den allgemeinen Cybersicherheitsmaßnahmen und Strafverfolgungsmaßnahmen als Reaktion auf Cybersicherheitsvorfälle. Die Kommission fordert die Mitgliedstaaten auf, derartige Initiativen zu erörtern und zu bewerten, wie qualifizierte Arbeitskräfte Cybersicherheitsgemeinschaften sowohl im Verteidigungswesen als auch im zivilen Bereich am besten zugutekommen können.

Die Kommission wird Überlegungen über Vorschläge zur Schließung der aktuellen und prognostizierten Lücken anstellen, die bei ihrer Überprüfung des Bedarfs der Organe, Einrichtungen und sonstigen Stellen der Europäischen Union ermittelt wurden. Sie wird insbesondere Arbeitskräfte darin bestärken, von dem im Rahmen des Dialogs zwischen der EU und den Vereinigten Staaten etablierten künftigen **Cybersicherheitsstipendium der EU und der Vereinigten Staaten** zu profitieren.

**Maßnahmen im Rahmen der Akademie**

**Wirtschaft**

- Vorschlagen konkreter **Cybersicherheitszusagen** auf der Plattform für digitale Kompetenzen und Arbeitsplätze ab dem 18. April 2023.

**Mitgliedstaaten**

- Aufnahme spezifischer Maßnahmen zur Schließung der Lücke bei

[79] Verordnung (EU) 2021/1057 des Europäischen Parlaments und des Rates vom 24. Juni 2021 zur Einrichtung des Europäischen Sozialfonds Plus (ESF+) und zur Aufhebung der Verordnung (EU) Nr. 1296/2013, Artikel 4 Absatz 1 Buchstabe c.

[80] NIS-2-Richtlinie, Artikel 7 Absatz 2 Buchstabe f.

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

Cybersicherheitskompetenzen in die **nationalen Cybersicherheitsstrategien**.

**Mitgliedstaaten und Wirtschaft**

- Umsetzung der Erklärung zu Frauen im Digitalbereich und Erreichen eines **ausgewogeneren Geschlechterverhältnisses in Cybersicherheitsberufen** bis 2030.

## 6. Finanzielle Förderung: Schaffung von Synergieeffekten zur Maximierung der Wirkung von Ausgaben für die Entwicklung von Cybersicherheitskompetenzen

Im Rahmen der Akademie wird die Wirkung von Investitionen in Cybersicherheitskompetenzen maximiert, indem eine gemeinsame Anlaufstelle bereitgestellt wird und der Einsatz von Mitteln besser auf den Marktbedarf abgestimmt und insgesamt optimiert wird, wobei Synergieeffekte zwischen verschiedenen Instrumenten erleichtert werden und zugleich Doppelarbeit vermieden wird.[82]

### *6.1. Anpassung der Mittel an den Bedarf*

Das Europäische Kompetenzzentrum für Cybersicherheit wird im Rahmen der Akademie mit Unterstützung der Kommission, des ECCO-Projekts und der nationalen Koordinierungszentren **Informationen darüber sammeln, wie EU-Mittel zur Finanzierung im Bereich Cybersicherheitskompetenzen eingesetzt werden**, und bewerten, inwiefern mit EU-Mitteln zur Verringerung der Lücke bei Cybersicherheitskompetenzen beigetragen wird. Unter Berücksichtigung dieser aggregierten Informationen wird sich das Europäische Kompetenzzentrum für Cybersicherheit um den gezielteren Einsatz von EU-Mitteln zur Deckung des ermittelten Bedarfs bemühen. Das Zentrum wird Maßnahmen zur Verringerung der am dringendsten zu schließenden Personallücken im Cybersicherheitsbereich fördern, einschließlich derjenigen im Zusammenhang mit der Deckung des cybersicherheitspolitischen Bedarfs.

### *6.2. Verbesserung der Sichtbarkeit verfügbarer Mittel und Partnerschaftsinitiativen für Cybersicherheitskompetenzen*

Die **Plattform für digitale Kompetenzen und Arbeitsplätze** wird kurzfristig zur zentralen Anlaufstelle für Interessenträger, bei der alle Informationen über Finanzierungsmöglichkeiten für Cybersicherheitskompetenzen verfügbar sein werden.

Die EU investiert in Menschen und deren Kompetenzen und nutzt Partnerschaften, insbesondere mit der Wirtschaft, um Maßnahmen zur Weiterbildung und Umschulung mithilfe mehrerer Instrumente zu mobilisieren, die im Rahmen der **Europäischen Kompetenzagenda**[83] identifiziert wurden, insbesondere mithilfe des **Kompetenzpakts**[84] und des **Aktionsplans für digitale Bildung**[85]. Mit dem **Programm „Digitales Europa“** werden Möglichkeiten zum Erwerb von Cybersicherheitskompetenzen – insbesondere im Rahmen von Initiativen für Mehrländerprojekte – finanziell gefördert. Dies ergänzt sich mit der durch

[82] Funding opportunities (europa.eu). Die Unterstützungsdienste des Kompetenzpakts bieten eine zentrale Anlaufstelle für Informationen über Finanzmittel für Kompetenzen, auch für das digitale Ökosystem. Zwar stellen die Unterstützungsdienste des Pakts allgemeine Informationen über Finanzierungsinstrumente bereit, die nicht speziell auf Cybersicherheitskompetenzen ausgerichtet sind, doch die Akademie sollte ihre Arbeit dennoch berücksichtigen, um Doppelungen zu vermeiden.

[83] Europäische Kompetenzagenda – Beschäftigung, Soziales und Integration – Europäische Kommission (europa.eu).

[84] EU-Förderung für Weiterbildung und Umschulung – Beschäftigung, Soziales und Integration – Europäische Kommission (europa.eu).

[85] Aktionsplan für digitale Bildung (2021-2027).

Horizont Europa angebotenen Unterstützung für Forschung und innovative technologische Lösungen im Cybersicherheitsbereich. Mit Mitteln des **Europäischen Verteidigungsfonds**[86] werden Forschung und technologische Entwicklung gefördert, damit effiziente Cyberoperationen durchgeführt werden, einschließlich Schulungen und Übungen[87]. Auch im Rahmen von **Erasmus+** werden solche Initiativen weiter unterstützt, u. a. durch gemischte Intensivprogramme und Kooperationsprojekte.

Die Mitgliedstaaten werden aufgefordert, die von ihnen direkt verwalteten EU-Mittel zur Unterstützung von Kompetenzen und Arbeitsplätzen im Cybersicherheitsbereich zu mobilisieren. Die Fonds der Kohäsionspolitik wie der **Europäische Fonds für regionale Entwicklung (EFRE)** und der **ESF+** bergen in diesem Zusammenhang ein erhebliches Potenzial für Synergieeffekte.[88] Bei den Maßnahmen im Rahmen der **Aufbau- und Resilienzfazilität** (ARF)[89] und von **InvestEU**[90] sind weitere wichtige Komplementaritäten bei der Verwirklichung der Ziele der Akademie möglich.

**Maßnahmen im Rahmen der Akademie**

**Europäisches Kompetenzzentrum für Cybersicherheit und ENISA**

- **Erfassung** der vorhandenen EU-Mittel für Cybersicherheitskompetenzen unter Berücksichtigung des Marktbedarfs, Bewertung der **Wirksamkeit** und Ermittlung von **Finanzierungsprioritäten** bis Ende 2024.

**Kommission**

- Schaffung einer **zentralen Anlaufstelle** für Finanzierungsmöglichkeiten für Cybersicherheitskompetenzen auf der Plattform für digitale Kompetenzen und Arbeitsplätze bis Ende 2023.

## 7. Messung der Fortschritte: integrierte Rechenschaftspflicht

Im Rahmen der Akademie wird eine **Methodik** entwickelt, mit der die **Fortschritte bei der Schließung der Lücke bei Cybersicherheitskompetenzen gemessen** werden können.

### *7.1. Festlegung von Cybersicherheitsindikatoren zur Überwachung der Entwicklung des Cybersicherheitsarbeitsmarkts*

[86] Verordnung (EU) 2021/697 des Europäischen Parlaments und des Rates vom 29. April 2021 zur Einrichtung des Europäischen Verteidigungsfonds und zur Aufhebung der Verordnung (EU) 2018/1092.

[87] Die Mitgliedstaaten haben sich zu gemeinsamen Schulungen und Übungen verpflichtet, beispielsweise durch die Einführung von Projekten für Cyberschulungen und -übungen im Rahmen der Ständigen Strukturierten Zusammenarbeit (SSZ) und die Teilnahme daran, darunter beispielsweise: EU Cyber-Akademie und Innovation Hub (EU CAIH) und Cyber-Range-Verbände.

[88] Artikel 3Absatz 1 der Verordnung (EU) 2021/1058 und Artikel 4 Absatz 1 Buchstabe g der Verordnung (EU) 2021/1057.

[89] Z. B. sind im estnischen Aufbau- und Resilienzplan Investitionen in digitale Kompetenzen (in Höhe von 10 Mio. EUR) vorgesehen. Unter anderem sollen hiermit Schulungen für IKT-Fachkräfte überarbeitet werden, die Weiterbildung und Umschulung von IKT-Fachkräften im Cybersicherheitsbereich soll finanziell gefördert werden, und es soll zur Entwicklung eines Pilotprogramms zur Umgestaltung des Qualifikationsrahmens für IKT-Fachkräfte beigetragen werden.

[90] Interessenträger (z. B. Schulungsanbieter und Unternehmen, die eigene Schulungsmaßnahmen im Cybersicherheitsbereich gestalten oder diese verbessern wollen) können sich an die InvestEU-Beratungsplattform wenden, die technische Unterstützung und Hilfe bietet, auch für den Kapazitätsaufbau bei Projektentwicklern und Einrichtungen, und sie können das InvestEU-Portal konsultieren.

Der **Index für die digitale Wirtschaft und Gesellschaft (DESI)** fasst Indikatoren zur digitalen Leistung Europas zusammen und ermöglicht es, die Fortschritte der EU-Mitgliedstaaten zu verfolgen. Im Rahmen der Akademie für Cybersicherheitskompetenzen wird die ENISA in Zusammenarbeit mit der Kommission und der NIS-Kooperationsgruppe[91] **Indikatoren** – darunter auch geschlechtsbezogene Indikatoren – entwickeln, um die Fortschritte der EU-Mitgliedstaaten bei der Erhöhung der Zahl der Cybersicherheitsfachkräfte zu verfolgen; dabei werden auch einschlägige Marktteilnehmer und die nationalen Koordinierungszentren konsultiert. Die ENISA wird sich auf die DESI-Methodik[92] stützen und dafür sorgen, dass die Indikatoren mit den europäischen Digitalzielen für IKT-Fachkräfte und für das Erreichen eines ausgewogeneren Geschlechterverhältnisses im IKT-Bereich vereinbar sind. Anschließend wird die Kommission darauf hinarbeiten, die Indikatoren in den DESI einzubeziehen, was die jährliche Verfolgung des Stands der Cybersicherheitskompetenzen und des Arbeitsmarkts ermöglicht.

### *7.2.Datenerhebung und Berichterstattung*

Die ENISA wird die Daten zu den Indikatoren mit Unterstützung des ECCO-Projekts und der nationalen Koordinierungszentren erheben. Auf der Grundlage der erhobenen Daten wird die ENISA einen **jährlichen Bericht** ausarbeiten, der zum Bericht über den Stand der digitalen Dekade[93] beiträgt, der wiederum zusammen mit dem DESI in die länderspezifischen Analysen und Empfehlungen im Rahmen des **Europäischen Semesters** einfließen wird[94]. Darüber hinaus werden die Indikatoren für Cybersicherheitskompetenzen zum in der NIS-2-Richtlinie vorgesehenen **zweijährlichen Bericht** der ENISA über den Stand der Cybersicherheit in der EU beitragen, in dem die Themen Cybersicherheitskapazitäten, Sensibilisierung für Cybersicherheit und Cyberhygiene in der gesamten EU abgedeckt werden.

### *7.3.Ausarbeitung wesentlicher Leistungsindikatoren für die Cybersicherheit*

Zur Schließung der Fachkräftelücke im Cybersicherheitsbereich in Europa wird die ENISA der Kommission in enger Zusammenarbeit mit der Kommission und den nationalen Koordinierungszentren wesentliche Leistungsindikatoren (KPI) vorschlagen und sich dabei auf die Methoden des Politikprogramms 2030 für die digitale Dekade und auf Erfahrungen der Wirtschaft stützen. Die ENISA wird die KPI, die die Mitgliedstaaten zur Bewertung ihrer nationalen Cybersicherheitsstrategien[95] heranziehen, gebührend berücksichtigen.

**Maßnahmen im Rahmen der Akademie**

**ENISA**

- Ausarbeitung von **Indikatoren und KPI** für Cybersicherheitskompetenzen bis Ende 2023.
- **Erhebung von Daten** über Indikatoren und Berichterstattung darüber (erste Erhebung bis 2025).

[91] Gestützt auf die Methodik, die die ENISA gemäß Artikel 18 Absatz 3 der NIS-2-Richtlinie für ihren zweijährlichen Bericht über den Stand der Cybersicherheit in der Union entwickeln muss, und ergänzend zu dieser Methodik.

[92] Siehe: Digital Economy and Society Index (DESI) 2022 – Methodological Note, verfügbar auf folgender Seite: The Digital Economy and Society Index (DESI) | Shaping Europe's digital future (europa.eu).

[93] Beschluss (EU) 2022/2481 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Aufstellung des Politikprogramms 2030 für die digitale Dekade.

[94] Ebd., Erwägungsgrund 25.

[95] NIS-2-Richtlinie, Artikel 7 Absatz 4.

**Kommission**

- Hinarbeiten auf die Einbeziehung von **Indikatoren für die Cybersicherheit in den DESI** und in den **Bericht über den Stand der digitalen Dekade**.

## 8. Fazit

Diese Mitteilung bildet die Grundlage für eine Überarbeitung des EU-Ansatzes zur Förderung des Erwerbs von Cybersicherheitskompetenzen durch Fachkräfte in der EU. Ziel ist es, die Lücke bei Cybersicherheitskompetenzen zu verringern und dafür zu sorgen, dass die EU über die benötigten Arbeitskräfte verfügt, um auf die sich ständig wandelnde Bedrohungslage reagieren und EU-Strategien zum Schutz der EU vor Cyberangriffen umsetzen, aber auch Geschäftsmöglichkeiten und die Wettbewerbsfähigkeit fördern zu können. Qualifizierte Arbeitskräfte im Cybersicherheitsbereich können Gemeinschaften **in der Zivilgesellschaft, im Verteidigungswesen, in der Diplomatie und in der Strafverfolgung** zugutekommen und Synergieeffekte zwischen ihnen erleichtern.

Die Kommission fordert die Mitgliedstaaten und alle Interessenträger auf, zur Verwirklichung der Ziele der Akademie für Cybersicherheitskompetenzen beizutragen.