Council of the European Union

Brussels, 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

COVER NOTE

From:	Secretary-General of the European Commission, signed by Ms Martine DEPREZ, Director
date of receipt:	19 April 2023
To:	Ms Thérèse BLANCHET, Secretary-General of the Council of the European Union
No. Cion doc.:	COM(2023) 207 final
Subject:	COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL **Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')**

Delegations will find attached document COM(2023) 207 final.

Encl.: COM(2023) 207 final

EUROPEAN
COMMISSION

Strasbourg, 18.4.2023
COM(2023) 207 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience
('The Cybersecurity Skills Academy')

Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience
('The Cybersecurity Skills Academy')

1. An urgent need to reduce risks by addressing the cybersecurity skills shortage and gaps

Cybersecurity is not only part of citizens, businesses, and Member States' security. It is also a necessity to ensure the EU's political stability, the stability of its democracies and the prosperity of our society and businesses. The cybersecurity **threat landscape** has evolved greatly in the past years, with the worrying trend that a growing number of cyberattacks target military and civilian critical infrastructure in the EU. Threat actors increase their capabilities and novel, hybrid and emerging threats, such as the use of bots and techniques based on artificial intelligence, are emerging[1]. Notably, ransomware threat actors are routinely inflicting considerable damage, both financially and reputationally, to entities[2].

A large number of cybersecurity incidents have also targeted public administration and governments in Member States, as well as European Institutions, Bodies and Agencies (EUIBAs)[3]. The finance[4] and health[5] sectors, both backbones of society and economy, have also consistently been targeted[6]. The geopolitical tensions linked to Russia's war of aggression against Ukraine have increased the cybersecurity threat[7] and have the potential of destabilising our society. The **security** of the EU cannot be guaranteed without the **EU's most valuable asset: its people.** The EU urgently needs professionals with the skills and competences to prevent, detect, deter and defend the EU, including its most critical infrastructures, against cyberattacks and ensure its **resilience**.

The cybersecurity talent gap further hampers Europe's **competitiveness** and **growth**, which heavily depend on the development and uptake of strategic digital technologies (e.g. artificial intelligence, 5G and cloud). A skilled cybersecurity workforce is needed in order for the EU to remain in a position to deliver key advanced technologies in a global setting.

To prepare for and to face this evolving threat landscape and to foster EU's competitiveness, the EU cybersecurity policy has progressed significantly in the last years leading to the

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

[2] Europol Internet Organised Crime Threat Assessment (IOCTA) 2021. Such actors build on the model of Ransomware-as-a-service. The annual cost to businesses exceeded EUR 18.4 billion in 2022 (Cybereason 2022 Report on the true cost or Ransomware).

[3] See for example Joint Publication by ENISA and CERT-EU, JP-23-01 - Sustained activity by specific threat actors, TLP:CLEAR, 15 February 2023.

[4] See for example in Germany, 90% of the mail fraud reported from 1 June 2021 to 31 May 2022 was finance phishing, or the attack on a company in the financial sector, involving more than 20,000 infected devices from 125 countries, The State of IT Security in Germany in 2022, Bundesamt für Sicherheit in der Informationstechnik (BSI), 1st of January 2023

[5] See for example in France, ransomware attacks on public healthcare facilities such as on the Centre Hospitalier Sud Francilien, during which 11GB of personal and medical data, as well as staff-related data was compromised and published by the threat actor, Panorama de la cybermenace 2022, Agence nationale de la sécurité des systèmes d'information (ANSSI), janvier 2023

[6] ENISA Threat Landscape 2022

[7] See also: CERT-EU – Russia's war on Ukraine: one year of cyber operations (europa.eu); Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union, 10 May 2022 ; Declaration by the High Representative on behalf of the European Union on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine, 19 July 2022.

adoption of a number of initiatives such as the EU's Cybersecurity Strategy for the Digital Decade[8], the revised Network and Information Security Directive (NIS2 Directive)[9], EU sectoral cybersecurity legislation[10], the EU policy on cyber defence[11], the Cyber Resilience Act[12] and the Cyber Solidarity Act, proposed by the Commission together with this Communication. But without the necessary skilled people to implement them, these pieces of legislation will not achieve their objectives. While the basic knowledge of cybersecurity by the general population is addressed as part of initiatives supporting the development of general skills needed to participate in society[13], a competent workforce is essential in both the public and private sector, at national and EU level, including in standardisation organisations, **to deliver on those cybersecurity legal and policy requirements.**

The EU's security and competitiveness therefore depend on having a professional skilled cybersecurity workforce. However, the EU is facing a very substantial shortage of skilled cybersecurity professionals, which puts the EU, its Member States, its businesses and citizens at risk of cybersecurity incidents. In 2022, the shortage of cybersecurity professionals in the European Union ranged **between 260,000**[14] **and 500,000**[15], while the EU's cybersecurity workforce needs were estimated at 883,000 professionals[16] , suggesting a misalignment between the competences available and those required by the labour market. The cybersecurity workforce further suffers from the misconception associated with its technical image, and continues to fail at attracting **women**, who amount to 20% of cybersecurity graduates[17] and to 19% of information and communications technology (ICT) specialists[18] To address this, Europe's **Digital Decade Policy Programme 2030**[19] has set the target of increasing the number of ICT professionals by 20 million by 2030, while also achieving gender convergence. Moreover, implementing emerging EU policy requires an adequately skilled and sufficient workforce. For example, over 42% of senior IT leaders in the financial services industry highlighted the lack of cybersecurity skills and expertise as a key challenge

[8] Joint communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, JOIN(2020) 18 final.

[9] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

[10] Such as, for the financial sector, Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (DORA regulation)

[11] Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final

[12] Proposal for a regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020, COM/2022/454 final

[13] Among the relevant initiatives addressing general digital skills for the population: 80% of the population reaching basic digital skills by 2030 as a target of the European Pillar of Social Rights Action Plan and the Digital Compass, the Digital Education Action Plan 2021-2027, the Digital Competence Framework tool, or the proposal for Council recommendation on improving the provision of digital skills in education and training.

[14] (ISC)² in Assessing Cyber Skills on the basis of the ECSF, ENISA webinar, 16 February 2023

[15] According to European Cyber Security Organisation (ECSO), as stated in the Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final

[16] (ISC²) in Assessing Cyber Skills on the basis of the ECSF, ENISA webinar, 16 February 2023

[17] Cybersecurity Higher Education Database (CyberHEAD)

[18] Only 19% of ICT specialists in the EU are women Digital Economy and Society Index (DESI) 2022 | Shaping Europe's digital future (europa.eu). No number is available regarding the Union's feminine cybersecurity workforce.

[19] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, which sets up a monitoring and cooperation mechanism to achieve the common objectives and targets for Europe's digital transformation set out in the 2030 Digital Compass, including the area of skills.

facing their business when it comes to cybersecurity defence and incident management[20], at a time when they will need to implement sectoral cybersecurity legislation such as the Digital Operational Resilience Act (DORA).

Employers' hesitancy to invest in human capital, looking for already trained and experienced workforce, further contributes to constraining the labour market[21]. This shortage affects all types of companies, including small and medium-sized enterprises (**SMEs**), which represent 99% of all businesses in the EU[22]. The challenge is also high for **public administrations** which are largely hit and most impacted by cybersecurity incidents[23].

Closing the EU's cybersecurity professional talent gap is therefore a matter of urgency, as the EU's security and competitiveness are at stake.

2. The lack of synergies and coordinated action to close the cybersecurity skills gap

Initiatives at European and national level conducted by public and private entities to address the cybersecurity labour market shortages are flourishing. However, they are scattered and have so far failed to reach a critical mass to make a real difference.

To start with, there is currently limited common understanding of the composition of the EU cybersecurity workforce and of associated skills, whereas similar cybersecurity job profiles should entail the same set of skills. The low uptake by relevant actors of a common **European reference framework for cybersecurity professionals** translates into the lack of a communication tool between employers, educators and policy makers, and incapacity to conduct measurement and assess the gaps of the cybersecurity labour market. It further prevents the design of education and training curricula and the creation of career pathways responding to the policy and market needs for those wishing to enter the profession. **Upskilling and reskilling** of the workforce relies widely on cybersecurity trainings and certificates, usually offered by private providers. However, the workforce faces difficulties to get an overview of the quality of the cybersecurity trainings offered and the associated certificates issued.

While education and training and building career pathways are necessary to enhance the supply side of the labour market, the role of the **demand side** in training its workforce and adapting to its evolution is currently underestimated. Industry and public employers lack common fora and places to pool ideas on how to best train the workforce and to address how to **better assess skills**, especially during the recruitment process. The most in-demand **hard skills** may be cybersecurity related[24], such as software development or cloud computing[25], but **transversal skills** are still unjustifiably disregarded. Critical thinking and analysis, problem-solving and self-management are skill groups which are more demanded by employers[26] and are rising in prominence in the lead up to 2025[27].

[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)

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

[25] ISACA State of Cyber Security 2022 infographic

[26] Such as the CEDEFOP tool: Skills-OVATE | CEDEFOP (europa.eu)

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

Many public and private investment initiatives in cybersecurity skills exist already, with the EU widely **funding** projects under different instruments[28]. However, the continuing shortage of skills in the EU raises questions as regards their visibility and impact and suggests that they may not systematically match the needs of the market, which need to be urgently mapped at EU level. In addition, several sources of funding lead to duplication, missing the opportunity to scale up and make a real impact. Moreover, those who need the investment cannot always identify the most appropriate sources for their needs.

Stakeholders have been trying to address the complex and multifaceted issue of the shortage of cybersecurity skills. The EU Agency for Cybersecurity (ENISA) has been developing instruments related to role profiles or higher education[29], the European Cybersecurity Competence Centre (ECCC)[30] is addressing cybersecurity skills in a dedicated working group, the European Security and Defence College (ESDC) is working on the cybersecurity skills of the civilian and military workforce in the context of the Common Security and Defence Policy[31], private organisations are trying to tackle the issue[32], the cybersecurity certification industry is developing a roadmap and trainings targeting the skills gap[33]. Member States are also trying to address the issue through a variety of initiatives, ranging from regulatory[34] to setting up of cybersecurity skills academies[35] or Cyber Campuses[36], Cybercrime Centres of Excellence[37], or through public-private partnerships[38]. However, the work of all these stakeholders often lacks coordination and synergies and has not reached its potential of making a substantial difference on the job market as shown by the growing shortage in the cybersecurity workforce in the EU. Increasing synergies across cyber communities is also needed as the necessary skillsets to uphold cybersecurity, fight **cybercrime** or build **cyber defence** responses are often of a similar nature.

Finally, today, the EU has limited means of assessing the **state and the evolution of the cybersecurity labour market** and of the skills of its workforce. Member States and EUIBAs rely on either data collected by private entities or on a wider set of EU-collected data notably by Eurostat[39] and the European Centre for the Development of Vocational Training (CEDEFOP)[40] on ICT professionals. In other words, the EU has a partial and fragmented

[28] For example: Cybersecurity Skills Alliance – New Vision for Europe – REWIRE project (funded by the Erasmus+ program); projects supporting the Cybersecurity Competence Centre (ECHO, CONCORDIA, CyberSec4Europe, SPARTA (funded by Horizon 2020), Cybersecpro project (funded by the Digital Europe Programme).

[29] Notably: the European Cybersecurity Skills Framework (ECSF); the CYBERHEAD - Cybersecurity Higher Education Database; the Cyber Exercise Platform (CEP); the European Cyber Security Challenge; the European Cyber Security Month.

[30] Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres

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

[32] For example, the European Cybersecurity Organisation (ECSO)'s Working Group 5 on "Education, training, awareness, cyber ranges, human factors"; the organisation DIGITALEUROPE

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

[34] For example, in national strategies for education or cybersecurity

[35] For example, the C-Academy in Portugal

[36] For example, Cyber Campuses in France

[37] For example, the Lithuanian Cybercrime Centre of Excellence for Training, Research & Education in Lithuania (L3CE)

[38] For example, Microsoft's Cybersecurity Skilling Initiative

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

[40] Such as the CEDEFOP tool: Skills-OVATE | CEDEFOP (europa.eu)

view of its needs, which prevents it from consolidating an aggregated vision of the state of the cybersecurity labour market.

3. An EU-wide coordinated response: the Cybersecurity Skills Academy

3.1. The objective

To overcome the challenge of addressing cybersecurity skills and closing the labour market gap, the Commission is putting forward a **Cybersecurity Skills Academy**, as announced by the President of the European Commission in her 2022 State of the Union Letter of Intent[41, 42], and in the context of the European Year of Skills.

The Cybersecurity Skills Academy (in short, 'the Academy') aims at creating a **single point of entry and synergies** for cybersecurity education and training offers as well as for funding opportunities and specific actions for supporting the development of cybersecurity skills. It will scale up stakeholders' initiatives to reach a critical mass that will make a difference on the labour market, including for defence. Those activities would align along common goals and key performance indicators to seek greater impact.

The focus of the Academy will be the skilling of **cybersecurity professionals**. The activity of the Academy will feed into to EU policies on cybersecurity, but also into education and lifelong learning. It complements the two Council recommendations related to digital education and skills proposed by the Commission at the same time as this Communication[43].

The Academy will rely on four pillars: (1) fostering **knowledge generation through education and training** by working on a common framework for cybersecurity role profiles and associated skills, enhancing the European education and training offer to meet the needs, building career pathways and providing visibility and clarity over cybersecurity trainings and certifications to enhance the supply side of the labour; (2) ensuring a better channelling and visibility over available **funding opportunities** for skills-related activities in order to maximise their impact; (3) calling stakeholders **to take action**; and (4) defining indicators to **monitor the evolution of the market** and be in a capacity to assess the effectiveness of their actions.

The implementation of the Academy will be supported by a EUR 10 million funding from the Digital Europe Programme (DEP)[44].

3.2. The Academy's governance

Ultimately, to provide an infrastructure that serves as **a single entry point** to foster cooperation between academia, training providers and industry, where the supply and the demand sides of the EU cybersecurity ecosystem could meet and be trained, the Academy could take the shape of a **European digital infrastructure consortium (EDIC)**[45]. This instrument would allow Member States to work jointly on closing the cybersecurity skills gap, as well as to closely cooperate with the Commission, ENISA and the European Cybersecurity Competence Centre (ECCC), in line with their mandates and competences, and

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

[42] Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final

[43] Proposals for Council recommendations on the key enabling factors for successful digital education and training, and on improving the provision of digital skills in education and training.

[44] Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240

[45] EDICs were established in the Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030, Article 13 et sq.

to bring on board all relevant stakeholders but also direct European, national and private investment into a common objective. For that purpose, interested Member States are encouraged to submit to the Commission a pre-notification by 30 May 2023 of their future application for such an EDIC. This voluntary pre-notification would allow the Commission to issue early comments on the draft EDIC application, thus allowing for its further development and formal submission in a speedier manner. During the entire process and to the extent requested by Member States, the Commission, acting as a multi-country project accelerator, will facilitate the preparation of the EDIC application. Then, upon a positive assessment of the application by the Commission and approval by the Digital Decade Programme Committee, the Commission would issue a Decision establishing the EDIC and subsequently help coordinate the implementation of the EDIC[46].

In the meantime, and while the EDIC is being formally set-up, the Commission will create a virtual single point of entry by enhancing the Commission's **Digital Skills and Jobs Platform**[47] with the support of the European Cybersecurity Community Support (ECCO) project[48].

ENISA will contribute to the implementation of the Academy in line with the agency's objectives[49], notably with regards to assistance in cybersecurity education and training, and taking into consideration its reporting obligations under the NIS2 Directive[50]. The **ECCC** will work in line with its Strategic Agenda to support the implementation of the Cybersecurity Skills Academy. Notably, the ECCC will implement Strategic Objective 3 (Cybersecurity) of the Digital Europe Programme. It will benefit from the support of the Commission and Member States, through the **National Coordination Centres (NCCs)**. The **Cooperation Group** established under the NIS2 Directive[51] will be solicited where relevant. Finally, joining forces with the **industry** and **academia** will be necessary to reach the Academy's goal of closing the cybersecurity skills gap.

4. Knowledge generation and training: establish a common EU approach to cybersecurity training

Under the knowledge generation and training pillar of the Cybersecurity Skills Academy, a structured approach will be developed with the clear objective to increase the **number** of persons with cybersecurity skills in the EU, to better target trainings to **market needs**, and provide visibility over **career pathways**.

4.1. Speaking the same language: a common approach on cybersecurity role profiles and associated skills

[46] ibid, Article 12

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

[48] See European Cybersecurity Competence Centre and Network: new EU-funded project to support the Cyber Community (europa.eu). In December 2022, the European Commission signed a contract of EUR 3 million to support the EU Cyber Community in the framework of European Cybersecurity Competence Centre. This project will contribute to EU's goals on community and capacity building regarding cybersecurity research, innovation, uptake and industrial base.

[49] "ENISA shall support capacity-building and preparedness across the Union by assisting the Union institutions, bodies, offices and agencies, as well as Member States and public and private stakeholders, (…) to develop skills and competencies in the field of cybersecurity." Article 4(3) of the Cybersecurity Act

[50] Article 18 of the NIS2 Directive

[51] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

Work has already been done by ENISA towards defining role profiles of cybersecurity professionals under the European Cyber Skills Competence Framework (**ECSF**)[52]. This should become the basis for the Academy to define and assess relevant skills, monitor the evolution of the skill gaps and provide indications on the new needs. For each cybersecurity role of the ECSF, a set of applicable European e-Competence Framework[53] is incorporated as an element of the profile description[54].

ENISA will therefore review the ECSF and **identify evolving skills needs and gaps** in the cybersecurity workforce, including through advanced tools (e.g. artificial intelligence, big data[55], data mining). For that purpose, ENISA will work under the steer of the EDIC, when established, the ECCC, together with NCCs, the Commission, the ECCO project, and market players[56]. For the cyber defence workforce, ENISA will take into due account the work done by the ESDC. Similarly, in the area of fighting cybercrime, ENISA will factor in the activities carried out by EU Agency for Law Enforcement Training (CEPOL) and Europol in establishing an Operational Training Needs Analysis[57] on cyberattacks.

The ECSF will be regularly complemented and reviewed under the Academy throughout a two-yearly cycle. In addition, the Commission and the European External Action Service will contribute to defining specific profiles and associated skills for sectors as needed, with the support of EU agencies and bodies, such as the ESDC[58], Europol and CEPOL[59].

Links will also be made between the ECSF and relevant instruments of EU employment policy[60]. In particular the ECSF job profiles as well as related skills will be integrated into the **ESCO classification**. This will improve the classification of and linkages between occupations and skills in the field of cybersecurity, making it easier for individuals to upskill and reskill and supporting skills-based job matching and cross-border mobility.

4.2. Fostering cooperation to design cybersecurity education and training curricula

Once the EDIC is set up, the Academy should receive support from Member States to become the **reference place in Europe for designing and delivering cybersecurity trainings** addressing the most in-demand skills and provide on-the-job trainings and traineeships opportunities for start-ups and SMEs and for public administrations in innovative

[52] European Cybersecurity Skills Framework (ECSF) — ENISA (europa.eu) The ECSF supports the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cybersecurity professionals. It summarises all cybersecurity-related roles into profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies.

[53] European e-Competence Framework (e-CF) | Esco (europa.eu) The e-CF provides consistent links in the context of ICT qualifications and other frameworks of relevance to the sector, amongst which DigComp

[54] See in this regard, User Manual - European Cybersecurity Skills Framework (ECSF) - September 2022.

[55] See for example, Skills-OVATE developed by Cedefop

[56] The agency will further leverage on results of other EU-funded projects (e.g. REWIRE, Data Space For Skills (DS4S), CyberSecPro, Concordia) and methodologies deriving from similar initiatives (e.g. e.g. "Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom and United States", OECD report, launched on 21 March 2023) to ensure in the future an up-to-date vision of the needs in an environment where the demand is constantly evolving.

[57] CEPOL Operational Training Needs Assessment (OTNA)

[58] See in this regard Joint Communication to the European Parliament and the Council, EU Policy on Cyber Defence, JOIN(2022) 49 final

[59] In this regard, attention will be paid to the work on the Cybercrime Training Competency Framework (TCF) currently under development.

[60] Such as the European Classification of Skills, Competences, Qualifications and Occupations (ESCO), Europass, the European cooperation network of employment services (EURES)

companies in cybersecurity and cybersecurity competence centres. The EDIC should work with all relevant stakeholders, including industry, to design such trainings, and build on projects such as **CyberSecPro**[61] funded by the Digital Europe Programme, which brings together 17 higher education institutions and 13 security companies from 16 Member States in order to become the best practice for all cybersecurity training programmes.

The Academy will work with all relevant stakeholders to **attract the young generations** to enter cybersecurity careers. In line with the proposal for a Council recommendation on improving the provision of digital skills in education and training, Member States should set up and reinforce measures to recruit and train specialised teachers and trainers and facilitate acquiring cybersecurity skills, including through apprenticeship placements. Integrating cybersecurity in education and training programmes, while ensuring their accessibility, developing the **apprenticeships** and traineeships offer, fostering innovative approaches including, for example, serious games and shared simulation platforms, organising immersion weeks in cybersecurity positions, explaining the non-technical role profiles should be encouraged. Participation in these cybersecurity learning opportunities of hard to reach groups, such as young people with disabilities, living in remote or rural areas and from other minority groups should also be supported.

Support will continue to be provided by the Commission for the development of micro-credentials, vocational education and training programmes. In particular, **joint bachelor and master degree programmes, joint courses or modules that can lead to micro-credentials** and **blended intensive programmes**[62] on all topics, including **on cybersecurity,** will continue to be financed under Erasmus+. The further rollout of the **European Universities Initiative**[63] and of **Centres of Vocational Excellence**[64] will also be supported to encourage greater cooperation between higher education and relevant vocational education and training institutions across Europe. EU funding programmes, including Erasmus+ and the Digital Europe Programme, will support this aim of deeper cooperation, as will EU funds for the development of **individual learning accounts**[65].

To facilitate cooperation at national level among academia and providers of cybersecurity skills trainings with private and public sector employers and foster synergies between the public and private sector, NCCs are invited to explore the setting up of **Cyber Campuses** in Member States. The Cyber Campuses would aim at providing poles of excellence at national level for the cybersecurity community and the Academy would help their networking and further coordination of their activities.

ENISA will also enhance its cybersecurity training offer aligning **its courses catalogue**[66] to the ECSF profiles and elaborating training modules per profile, which may enhance Member States training offers. ENISA will also expand its '**train the trainer' programme**[67],

[61] CyberSecPro It will, for example, conduct an analysis of the cybersecurity programmes, courses and summer schools offered in the universities and the European Credit Transfer and Accumulation System (ECTS) grading tables used, ensure the engagement of the target number of more than 530 trainees over the 3-year period, train external people from various industries and sectors

[62] Blended intensive programmes combine online teaching with a short period of physical mobility.

[63] European Universities initiative | European Education Area (europa.eu)

[64] Centres of Vocational Excellence | Erasmus+ (europa.eu)

[65] In line with the Council Recommendation of 16 June 2022 on individual learning accounts

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

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

targeting the professional needs of EUIBAs, and Member States' public authorities and **public and private critical operators** in the scope of the NIS2 Directive.

In addition, other EU agencies and bodies will strengthen their cybersecurity training offer. For example, implementing the EU policy on cyber defence, the **ESDC** will develop a new set of cybersecurity courses and will align some of its current courses with the ECSF. These courses will lead to certification of learning outcomes[68]. The ESDC, in collaboration with the Commission, will explore the possibility of integrating certificates into the EUeID Wallet. The ESDC will further explore possible assessment of skills mechanisms, against which the certificates will be delivered. Similarly, in the area of fighting cybercrime, close connections with the **CEPOL Cybercrime Academy**[69] will be sought to foster synergies and complementarities in the design and implementation of training curricula.

4.3. Creating synergies and providing visibility to cybersecurity trainings and certification across Member States

The Academy should address the issue of visibility and synergies of training and certification. This would benefit the civilian, defence, law enforcement and diplomatic cyber communities, as all sectors require in many cases the same expertise, based on similar curricula and learning outcomes.

The Academy would provide a **single point of entry** for those interested in a cybersecurity career. In the short term this will be done by enhancing the Commission's **Digital Skills and Jobs Platform** with the support of the ECCO project. A specific section to cybersecurity careers, will link with existing tools, from higher education programmes to training opportunities, including courses leading to micro-credentials and vocational education and training programmes, to job offers. This will be achieved by referring to or integrating into the platform ongoing work and initiatives, such as the ones of ENISA, who in collaboration with academia has set up a **mapping of education institutions** providing cybersecurity programmes. This will be further enhanced with the support of NCCs. In addition, two **repositories of existing trainings from public and private sectors and of cybersecurity certifications** will be developed and consolidated by ENISA with the support of NCCs, the Commission and the ECCO project, and in collaboration with entities delivering certifications and drawing also on other relevant initiatives[70]. These will also be integrated into the single point of entry of the Digital Skills and Jobs Platform. This work will also benefit NCCs whose task is notably to promote and disseminate cybersecurity educational programmes[71].

It is also necessary to provide assurances to professionals that the trainings they undertake are of the required quality. In this regard, ENISA will develop a **pilot project**, exploring the set-up of a European attestation scheme for cybersecurity skills.

In addition, identifying skills and trainings, and associating them with a job profile is

[68] In line with Article 20(4) of the Council Decision (CFSP) 2020/1515 of 19 October 2020 establishing a European Security and Defence College, and repealing Decision (CFSP) 2016/2382

[69] The CEPOL Cybercrime Academy has been established in 2019 to provide a state-of-the-art platform to improve cybercrime knowledge and cyber capacities in Europe.

[70] For example, the W4C Academy - Women4Cyber or the Global Cybercrime Certification project for Law Enforcement and Judicial Authorities

[71] "1. The national coordination centres shall have the following tasks: (…) (g) without prejudice to the competences of Member States for education and taking into account the relevant tasks of ENISA, engaging with national authorities regarding possible contributions to promoting and disseminating cybersecurity educational programmes", Article 7(1)(g) of the ECCC Regulation. See also associated recital 28.

essential, but it is also important to ensure that cybersecurity services are provided with the requisite competence, expertise and experience This is particularly the case for managed security services providers in areas such as incident response, penetration testing, security audits and consultancy. The NIS2 Directive and the Cyber Solidarity Act proposal set out specific tasks for such managed security services providers. Therefore, the Commission is also proposing a **targeted amendment to the Cybersecurity Act**[72] to enable certification schemes of managed security services at EU level. Such certification schemes should aim at, inter alia, ensuring that these services are provided by staff with a very high level of technical knowledge and competence in the relevant areas.

Quality assurance and recognition mechanisms for micro-credentials[73] facilitate the transparency, comparability and portability of learning outcomes. In line with the Council recommendation on a European approach to micro-credentials[74], Member States are encouraged to include cybersecurity micro-credentials in their national qualification frameworks. That would allow them to relate the cybersecurity micro-credentials to the European Qualifications Framework[75]. The European Digital Credentials for Learning infrastructure is available to issue digitally signed cybersecurity qualifications and micro-credentials of individuals. These contain rich data including on cybersecurity learning outcomes and can be stored in the future **EUeID digital wallet**[76].

Actions under the Academy

Member States and industry

- Ensure the support for the development and recognition of cybersecurity learning **micro-credentials**, in line with the Council recommendation on a European approach to micro-credentials.
- Include cybersecurity qualifications, including micro-credentials in **National Qualifications Frameworks.**
- Provide **on-the-job learning opportunities** through apprenticeships for people going through cybersecurity skills development initiatives.

Commission

- In the short term, create **a single point of entry** for cybersecurity programmes, existing trainings, and for cybersecurity certifications via the **Digital Skills and Jobs Platform** by end of 2023.
- Propose an amendment to the **Cybersecurity Act** to allow the certification of managed security providers on 18 April 2023.

EU bodies and agencies

[72] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)

[73] For example, record or certificates of learning outcomes that people acquire following small trainings

[74] Council Recommendation on a European approach to micro-credentials for lifelong learning and employability

[75] Council Recommendation of 22 May 2017 on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on the establishment of the European Qualifications Framework for lifelong learning

[76] Proposal for a regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity

- Establish the **ECSF** as a common approach on cybersecurity role profiles and associated skills by end 2023.
- ENISA to initiate the development of a pilot project setting up a **European attestation scheme** for cybersecurity skills in Q2 2023.
- ENISA to review its **courses catalogue** and open its '**train the trainer' programme** to public and private critical operators by end 2023.
- Finish the **alignment of ESDC curricula with the ECSF** by mid-2023.

5. Stakeholder involvement: committing to close the cybersecurity skills gap

Under the Academy, a coordinated approach to stakeholder involvement will be developed to address the cybersecurity skills gap. The aim will be to maximise the visibility and impact of the various stakeholders' commitments aiming at narrowing the cybersecurity skills gap.

The Commission calls on stakeholders to make concrete commitments through pledges to upskill and reskill workers through dedicated actions, building as much as possible on the identified cybersecurity skills gap. Such **stakeholder cybersecurity pledges** should be reported on the **Digital Skills and Jobs Platform**, similarly to other digital pledges already visible on the platform. The Commission further encourages stakeholders making a cybersecurity pledge on the Platform to join the **Digital Large Scale Partnership under the Pact for Skills**[77]. Cybersecurity commitments made under the Digital Large Scale Partnership are encouraged to be submitted on the Digital Skills and Jobs Platform. Likewise, commitments made under the Digital Skills and Jobs Platform are encouraged to be reported under the Pact for Skills' Digital Large Scale Partnership.

The Commission further calls upon Member States to **pursue efforts in implementing the Women in Digital Declaration**[78] to encourage women to play an active and prominent role in the digital technology sector and achieve gender convergence in cybersecurity positions. The Commission also encourages Member States to develop synergies with their **European Social Fund+** (ESF+) programmes to further support the objective of gender equality in labour participation[79], for example through establishing **mentorship programmes for girls and women.** These can facilitate the building of role models to attract girls to cybersecurity professions, combatting at the same time gender-related stereotypes. It also encourages the upskill and reskill of women and fosters the development of a community, which can support women in their entry or promotion on the cybersecurity job market.

Member States should adopt, as part of **their national cybersecurity strategies, specific measures in view of mitigating the cybersecurity skills shortage**[80], identifying and better channelling efforts to close the skills gaps and ultimately ensuring a proper implementation of their obligations under the NIS2 Directive.

[77] New European Partnerships launched to deliver on the EU's ambitions for the Digital Decade | Shaping Europe's digital future (europa.eu), formed under the Pact for Skills to tackle the shortage of Information and Communication Technology (ICT)

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

[79] Regulation (EU) 2021/1057 of the European Parliament and of the Council of 24 June 2021 establishing the European Social Fund Plus (ESF+) and repealing Regulation (EU) No 1296/2013, Article 4(1)(c)

[80] NIS2 Directive, Article 7(2)(f)

Some Member States make use of **synergies between civilian, defence and law enforcement** initiatives. For example, growing a workforce using their national compulsory military service, or making use of cyber reservists, who are military-trained citizens filling in cybersecurity positions in the armed forces[81], allow the population, and especially young adults, to increase their cybersecurity and cyber defence skills. The same applies in the area of **fighting cybercrime** as many similarities exist between general cybersecurity efforts and law enforcement activities in the response to cybersecurity incidents-. The Commission encourages discussions amongst Member States on such initiatives and invites them to assess how a skilled workforce can best serve both the defence and civilian cybersecurity communities.

The Commission will reflect upon proposals on how to fill the current and anticipated gaps identified in its review of EUIBAs needs. It will in particular encourage staff to benefit from the forthcoming **EU-United States (US) cybersecurity fellowship** established under the EU-US dialogue.

Actions under the Academy

The industry

- Propose specific **cybersecurity pledges** on the Digital Skills and Jobs Platform as of 18 April 2023.

Member States

- Include in the **national cybersecurity strategies** specific measures to address the cybersecurity skills gap.

Member States and industry

- Implement the Women in Digital Declaration and achieve **gender convergence in cybersecurity positions** by 2030.

6. Funding: build synergies to maximise the impact of spending for developing cybersecurity skills

Under the Academy, the impact of investments into cybersecurity skills will be maximised by providing a common entry point, facilitating a better channelling of the funds towards the needs of the market and mainstreaming the use of funding, facilitating synergies between different instruments while avoiding duplication of efforts[82].

6.1. Matching the funds with the needs

Under the Academy, the ECCC, with the support of the Commission, the ECCO project and NCCs, will gather **information on how EU funds are used to finance cybersecurity skills**, and will assess how EU funds are supporting the narrowing of the cybersecurity skills gap. Taking into consideration this aggregated information, the ECCC will seek to ensure better

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

[82] Funding opportunities (europa.eu) The Pact for Skills Support services provide a single-entry point for skills funding information including for the Digital Ecosystem. The Pact Support Services provide generic information on funding instruments that are not specifically targeting cybersecurity skills, notwithstanding their work should be taken into account by the Academy to avoid duplication.

channelling of EU funds towards the identified needs. It will fund actions that would address the most pressing gaps in the cybersecurity workforce, including those related to the implementation of cybersecurity policy needs.

6.2. Providing visibility to available funds and partnership initiatives for cybersecurity skills

In the short term, the **Digital Skills and Jobs Platform** will become the single point of entry for stakeholders where all information on funding opportunities for cybersecurity skills will be available.

The EU is investing in people and their skills and using partnerships notably with the industry to mobilise action on up- and reskilling through several instruments identified under the **European Skills Agenda**[83], in particular the **Pact for Skills**[84] and the **Digital Education Action Plan**[85]. The **Digital Europe Programme** funds cybersecurity skills opportunities, notably through multi-country project initiatives, in clear complementarity with the support offered by Horizon Europe for research and innovative technological solutions in cybersecurity. The **European Defence Fund**[86] finances research and technology development to conduct efficient cyber operations, including trainings and exercises[87]. **Erasmus+** will continue to support such initiatives including through blended intensive programmes and cooperation projects.

Member States are encouraged to mobilise the EU funds they directly manage to support cybersecurity skills and jobs. The cohesion policy funds, such as the **European Regional Development Fund (ERDF)** and the **ESF+** carry important potential for synergies in this regard[88].The scope of actions under the **Recovery and Resilience Facility** (RRF)[89] and **InvestEU**[90]include further key complementarities in delivering the objectives of the Academy.

Actions under the Academy

European Cybersecurity Competence Centre and ENISA

- **Map** existing EU funding for cybersecurity skills against market needs, assess **effectiveness** and identify funding **priorities** by end of 2024.

[83] European Skills Agenda - Employment, Social Affairs & Inclusion - European Commission (europa.eu)

[84] EU funding instruments for upskilling and reskilling - Employment, Social Affairs & Inclusion - European Commission (europa.eu)

[85] Digital Education Action Plan 2021-2027

[86] Regulation (EU) 2021/697 of the European Parliament and of the Council of 29 April 2021 establishing the European Defence Fund and repealing Regulation (EU) 2018/1092

[87] Member States are committed for joint trainings and exercises, for example through establishing and participating in Permanent Structured Cooperation (PESCO) cyber trainings and exercises projects such as EU Cyber Academia and Innovation Hub (EU CAIH) and Federated Cyber Ranges.

[88] Regulation (EU) 2021/1058 Article 3(1) and Regulation (EU) 2021/1057 Article 4(1)(g)

[89] For example, the Estonian Recovery and resilience Plan foresees investment (10 MEUR) on digital skills will include the revision of trainings available to ICT experts, fund upskilling and retraining of ICT specialists in cybersecurity and will contribute to the development of a pilot programme to redesign the qualification framework for ICT specialists.

[90] Stakeholders (e.g. training providers and companies looking to design or improve their cybersecurity training activities) can approach the InvestEU Advisory Hub, that provides technical support and assistance including capacity building to project developers and entities, and consult the InvestEU Portal.

Commission

- Create a **single point of entry** for funding opportunities for cybersecurity skills on the Digital Skills and Jobs Platform by end of 2023.

7. Measuring progress: built-in accountability

Under the Academy a **methodology** will be developed that will allow **measuring the progress to close the cybersecurity skills gap**.

7.1. Defining cybersecurity indicators to monitor the evolution of the cybersecurity labour market

The **Digital Economy and Society Index (DESI)** summarises indicators on Europe's digital performance and tracks the progress of EU Member States. Under the Cybersecurity Skills Academy, ENISA, in cooperation with the Commission and the NIS Cooperation Group[91] will develop **indicators,** including related to gender, to track the progress made in EU Member States to increase the number of cybersecurity professionals, consulting also relevant market players and the NCCs. ENISA will draw on the DESI methodology[92] and will ensure that the indicators are in line with Europe's digital targets on ICT professionals and on achieving gender-convergence in ICT. The Commission will then work towards integrating such indicators into the DESI**,** thereby allowing for the yearly tracking of the state of the cybersecurity skills and job market.

7.2. Collecting data and reporting

ENISA will collect the data on the indicators with the support of the ECCO project and of the NCCs. Based on the data collected, ENISA will produce a **yearly report** that will contribute to the state of the Digital Decade Report[93], which, together with DESI, will further feed into the **European Semester** country-specific analysis and recommendations[94]. Moreover, the indicators on cybersecurity skills will contribute to ENISA's **two-yearly report** on the state of cybersecurity in the EU foreseen in the NIS2 Directive, covering cybersecurity capabilities, awareness and hygiene across the EU.

7.3. Preparing key performance indicators (KPIs) for cybersecurity

With the view of closing the European cybersecurity talent gap, ENISA, in close cooperation with the Commission and the NCCs will propose KPIs to the Commission, drawing on the methodology from the Digital Decade Policy Programme 2030, as well as on experience of the industry. ENISA will take into due account the KPIs used by Member States to assess their national cybersecurity strategies[95].

Actions under the Academy

[91] Drawing on and complementing the methodology to be developed by ENISA for the purposes of the agency's biennial report on the state of cybersecurity in the Union pursuant to Article 18(3) of the NIS2 Directive.

[92] See Digital Economy and Society Index (DESI) 2022 Methodological Note, available at The Digital Economy and Society Index (DESI) | Shaping Europe's digital future (europa.eu)

[93] Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the Digital Decade Policy Programme 2030

[94] Ibid, recital 25

[95] NIS2 Directive, Article 7(4)

ENISA

- Prepare **indicators and KPIs** on cybersecurity skills by the end of 2023.
- **Collect data** on indicators and report on them, with a first collection by 2025.

Commission

- Work towards the integration of **indicators on cybersecurity into DESI** and into the **state of the Digital Decade Report**.

8. Conclusion

This Communication sets the foundations for a revamp of the EU's approach to boosting cybersecurity skills for professionals in the EU. The aim is to reduce the cybersecurity skills gap and to equip the EU with the necessary workforce to allow it to respond to the constantly evolving threat landscape, implement EU policies that are aimed at shielding the EU from cyberattacks, but also to boost business opportunities and competitiveness. A skilled cybersecurity workforce can benefit the **civilian, defence, diplomatic and law enforcement** communities, facilitating synergies amongst them.

The Commission calls on Member States and all stakeholders to deliver on the ambition of the Cybersecurity Skills Academy.