Skills shortage puts Europe’s cyber resilience to the test

https://eurac.tv/9Wqa
Regulatory compliance, the disruption of Artificial Intelligence and international competition are just some issues regarding the lack of cyber skills in Europe and beyond.

Cybersecurity is an increasingly horizontal and urgent topic for policymakers, public authorities and industry practitioners in Europe. But as public bodies and private companies seek to upgrade their cybersecurity capacity, another problem emerges; the lack of relevant skills.

The EU has been working on a comprehensive set of cybersecurity laws, the Cybersecurity Act, the new Networks and Information Security Directive (NIS2) and the Cyber Resilience Act. However, lacking IT expertise might prevent companies and public authorities from implementing them in full.

At the same time, the impact of powerful AI models like ChatGPT is revolutionising the IT sector, as many tasks are increasingly automated. However, generative AI also opens the door for more cyber threats by facilitating actors in phishing and malware creation.

To what extent is the EU ready to face these challenges, what is the magnitude of the cyber skills gap compared to other countries and what more can be done to bolster capacity building are all questions that urgently need an answer.
Cyber skills gap keeps widening, report warns
EU seeks to bridge cyber-skills gap with new ‘academy’
Skills shortage puts Europe’s cyber resilience to the test
Cybersecurity sector braces for tug-of-war over AI
AI the next big challenge for the digital skills gap, EU’s Schmit says
Only business unusual will help Europe fill the cyber skills gap
A report by cybersecurity organisation (ISC)² suggests that the cyber skills gap is growing faster than it is being filled and that Europe might become an international laggard as technological trends and upcoming regulations make securing a cyber workforce ever more pressing.

The cybersecurity workforce gap analysis by (ISC)², a non-profit group, revealed that the demand for skilled cybersecurity professionals is growing faster than the workforce pool. The analysis revealed that Europe, the Middle East and Africa (EMEA) lack 317,050 cybersecurity professionals.

This is equivalent to an increase of approximately 60% over a year. To put this in perspective, the 2022 Global Cybersecurity Workforce Gap increased by 26% compared to the previous year.

Compared to other regions, the EMEA region displays the greatest increase in the cyber talent gap.

Reasons for the steep increase in demand for cybersecurity are the introduction of new technologies like Artificial Intelligence or quantum computing and the trend by companies to switch to more digital tools, which need cyber protection.

"The shortage of skilled professionals could expand further with the upcoming regulatory framework," an ENISA Spokesperson told EURACTIV. [Gorodenkoff / ShutterStock]
The mismatch also indicates a lack of management and oversight, which heightens the risk of cyberattacks in EU organisations, which cannot defend themselves against cybercrime properly.

Geopolitical tensions related to the Russian invasion of Ukraine only worsened this lack of preparation.

Another reason for the rise in the cyber skill talent gap is the introduction of new policies that will require more skilled professionals in this field.

According to the EU’s Agency for Cybersecurity, ENISA, the number of cyber-skilled professionals needed is expected to increase with the revised Networks and Information Directive (NIS2) introducing specific obligations for entities considered essential or important for society.

“The shortage of skilled professionals could expand further with the upcoming regulatory framework,” an ENISA spokesperson told EURACTIV.

The European Commission’s response to this skills gap was the Cyber Skills Academy, meant to bring together the different public and private initiatives for retraining the workforce and measure their aggregate impact.

Other initiatives include the European Skills Pact to match skills and the labour market more accurately and a database to search and find cybersecurity programmes offered by Higher Education Institute (CyberHEAD).

The EU in global comparison

In a separate report, (ISC)² analysed the cybersecurity policies and approaches of the EU, the UK, the US, Canada, Japan, and Singapore to understand the dynamics of the workforce gap in cybersecurity, estimated at around 3.4 million people worldwide.

The study found that the different jurisdictions adopted similar initiatives, especially to retain young individuals in cybersecurity professions. The report also pointed out that initiatives generally lack clarity in their obligations and effectiveness, particularly if they are non-binding.

The skill shortage reflects limitations of education, training systems, and policies to encourage and prepare the needed cyber professionals. Common barriers to cyber participation include a lack of basic digital skills and financial hurdles.

“The current training provision may need more flexibility to respond to rapidly changing skills needs in the sector and to be accessible to a diverse group of learners,” the report stated.

The case of Germany

A study by the German Economic Institute released in February estimated that the shortage of qualified workers in digitisation, of which cybersecurity experts are a part, could reach almost 106,000 people by 2026.

Likewise, for roughly every second vacancy, there were no suitably qualified unemployed individuals nationwide in 2021. By 2026, the percentage is expected to rise by another 23%.

To change these dynamics by facilitating entry into the field of cybersecurity and attracting workers from abroad, Germany launched initiatives such as MINT-Nachwuchs and Make it in Germany.

“The situation is expected to change only slowly, as changes in the education system only have a medium- to long-term effect,” explained Vera Demary, a digital expert at German Economic Institute.

On top of that, in Germany, education is the responsibility of the federal states. It makes it harder to introduce identical measures as the educational landscape differs from region to region, and German schools do not have the same priorities nationwide.

Alexander Müller, one of the liberals from the FDP party, who proposed a change in recruitment policy for the German armed forces last Friday (28 April), suggested that the approach needs to be multi-dimensional.

“On the one hand, we need to provide the best educational and training prospects, and on the other, we need to open the public sector to new employment models,” Müller told EURACTIV.
The European Commission launched Cybersecurity Skills Academy on Tuesday (18 April) to close the cybersecurity sector’s ongoing skills shortage and develop the EU’s cyber resilience.

The Cybersecurity Skills Academy is part of the 2023 European Year of Skills, an initiative to promote the upskilling and reskilling of the workforce with the view of helping workers and companies keep up with the green and digital transitions.

“500 million cybersecurity experts are missing in the coming years. We need the people to make it happen,” Commission Vice-President Margaritis Schinas told the hemicycle of the European Parliament gathered in Strasbourg on Tuesday (18 April).

“The academy aims to accelerate our efforts. It is a single point of entry for cybersecurity training and funding opportunities,” he added.

The academy is intended to fill in the cyber talent gap, as Europe is in dire need of IT experts to increase its resilience, as ENISA, the EU cybersecurity agency, told EURACTIV that in 2022 the shortage of cybersecurity professionals in the European Union ranged between 260,000 and 500,000. The platform recognises several certification schemes like (ISC)² and NVIDIA.

“Cybersecurity is a growing concern for everyone. Yet, there is still limited understanding on how to protect ourselves in practice – limited experts pool, no long experience managing cybersecurity...
risks, and ever-evolving technology and threat landscape have created a gap,” Iva Tasheva, cybersecurity lead at the consultancy CYEN, told EURACTIV.

**Cybersecurity Skills Gap**

The 2022 Digital Economy and Society Index (DESI), which tracks year-on-year progress towards the goals across EU countries, found that the current geopolitical context with Russia’s invasion of Ukraine “renders the implementation of innovative digital solutions, technologies, and infrastructures based on EU’s values and principles, as well as strengthening cybersecurity, even more relevant.”

Policymakers and industry practitioners are also concerned with the issue of ‘cyber poverty’. In a situation where a qualified cyber workforce is scarce, only large corporations can afford cyber teams, whilst smaller companies face the challenge of lacking cybersecurity training resources.

“We get to the point where being privacy and security conscious as individuals is really the domain of the wealthy and technical elite,” Patrick Wheeler, director of the workforce development program CyberWayFinder, told EURACTIV.

“Throwing bodies at this problem without improved societal aspects is a recipe for failure,” he added.

**New initiative**

With the new initiative, the Commission intends to contribute to narrowing the gap between needed and available skilled workers by providing means for specific training and further education programmes.

“Initiatives such as the EU Cybersecurity Skills Academy are steps in the right direction from policymakers to reduce the digital skills gap through education and training at all ages. This is a huge multi-faceted challenge that requires bringing all stakeholders at the table together,” Chris Gow, head of EU public policy at Cisco, told EURACTIV.

The Cyber Skills Academy is built on four pillars. The first pillar addresses education and training to foster EU cybersecurity knowledge. As part of the second pillar, it will also provide information on certification capacity and visibility on funding opportunities.

The third pillar includes stakeholder involvement, and the fourth will monitor the evolution of market developments and the cybersecurity skill gap by introducing a methodology on quality and intensity.

“A multi-stakeholder approach to funding opportunities is indispensable. The approach seems transparent and interactive.” Julia Schuetze, project director for cybersecurity policy at the think tank Stiftung Neue Verantwortung (SNV), told EURACTIV.

“Now, the new task lies in community management and coordination with third parties from academia, NGOs, and the Tech-community,” she added.

While the initiative might contribute to solving the problem, the Academy will not be a universal remedy, warns Philipp Eckhardt, a Centre for European Policy research officer.

“The establishment of a cybersecurity skills academy is ultimately a drop in the ocean,” he said.

**Goals for 2030**

The European Commission set the goal of reaching 80% of adult EU citizens with basic digital skills and 20 million employed Information and communications technology (ICT) specialists by 2030.

To attain the goals, efforts must be made regarding targeting current initiatives at educational institutions that focus on the working class under 30.

Wheeler of Cyberwayfinder noted how most mid-career switches that allow people to get IT training is internal programmes of ‘wealthy’ corporations, whilst new university graduates face steep challenges in landing their first cybersecurity job.

The challenge the new Initiative aims to address is to raise the level of cybersecurity knowledge of the existing workforce and citizens, regardless of their current professional activities.

“Even the retired or aged people need cybersecurity knowledge and awareness if they use digital services through a connected device,” ENISA told EURACTIV.

As education remains a national competence, member states bear the main responsibility to achieve the set 2030 goals.

“The EU can only play a supporting role here,” concludes Eckhardt.
A new regulatory framework to increase cybersecurity resilience is falling into place at the EU level, but it risks exposing the growing shortage of cyber-talent in regulators and companies.

A number of new regulatory requirements are set to enter into force with the revised Networks and Information Security Directive (NIS2) and the Cyber Resilience Act, which will set security standards for connected devices.

Cybersecurity company Fortinet published its 2023 Cybersecurity Skills Gap Global Research Report, which finds that "organisations are fighting an uphill battle against cyberthreat — incurring more breaches, in need of skilled professionals, and continuing to struggle to fill key positions," with 68% reporting they face additional risks because of skills shortages.

"A high number of leaders also attribute those breaches, at least in part, to a lack of cybersecurity skills among IT professionals," the report states.

But the situation is unlikely to improve soon, as more EU rules mean more demand for skilled professionals.

"The already existing shortage of skilled workers will increase in the future – not only due to the rightly increasing regulatory requirements, especially in the area of critical infrastructures, but above all due to an increase in the threat situation in cyberspace," Hans-Wilhelm Dünn, President Cyber Security Council Germany told EURACTIV.
Regulatory compliance

As for finding skilled employees who will be able to take the new regulations in their stride, “Cybersecurity experts in Europe are difficult to find and difficult to retain. The competition for talent is global and large companies with big budgets can afford the best people in this tight market,” European Cybersecurity Organisation’s (ECSO) Secretary General, Luigi Rebuffi, told EURACTIV.

To counteract the increasing gap, ECSO supports companies in recruiting cybersecurity experts through its HR community at the EU level. “Women4Cyber”, an ECSO sister organisation, has set up an academy for women and men to access the best cybersecurity training.

Similarly, ENISA, the EU’s agency for cybersecurity, has introduced a Cybersecurity Skills Framework that is a hands-on tool to identify tasks, competencies, skills and knowledge related to the roles of EU cybersecurity professionals. The agency also plans to propose a pilot skill attestation scheme.

“With these and other similar initiatives, we will be able to bridge the skills gap in Europe,” Rebuffi explained.

Pressure on regulators

While EU regulations are set to upgrade Europe’s cyber resilience, they put great pressure on national regulators like the Romanian National Cyber Security Directorate (DNSC), who have been forced to step up their game.

“Here at the DNSC, we worked tirelessly to recruit new specialists and guarantee we can compete with the private sector for these experts,” Mihai Rotariu, Mihai Rotariu, communications manager at the DNSC, told EURACTIV.

To cope with the insufficient national cybersecurity measures, Romania passed the Emergency Ordinance in September 2021 to boost the directorate’s operational capacity.

As a result, the DNSC is now “a civil cybersecurity authority with a much wider range of responsibilities than the previous institution,” Rotariu explained, noting a workforce of 1,250 people and counting.

Further steps to overcome the cybersecurity gap included passing two additional laws on the remuneration of personnel paid from public funds to attract more cybersecurity specialists in the public sector and another one on Romania’s security and cyber defence.

Self-reinforcing gap

In countries like Germany, the cybersecurity talent gap can also be traced back to the national educational system, which lacks a standardised approach for elementary and secondary schools.

“In education, increasing digitisation must be accompanied by cybersecurity awareness. We need more training in STEM [science, technology, engineering, and mathematics] subjects to steer graduates into this industry of the future,” Dünn told EURACTIV.

At the same time, the shortage of cyber staff might also be self-reinforcing, as the lack of enough workers means the stress level in the jobs of IT security officers are much higher than in other sectors, causing workers to look elsewhere, despite high levels of job security.

“Many IT security experts want to change their job field because pressure, stress, and a lack of work-life balance lead to an exceptionally high workload,” Dünn added.

An approach to counteract the skills gap would be impactful if employers shifted their focus away from applicants with bachelor’s and master’s degrees and instead hired staff with cyber skills and abilities.

This approach would reduce the cybersecurity skill gap and the number of individuals on the dark net who earn their living there due to a lack of adequate integration into society.

“With this triad of an education offensive, a changed corporate culture and a financial upgrade of the cybersecurity sector, the shortage of skilled workers can at least be mitigated,” Dünn concluded.
The continued development of AI brings both challenges and opportunities to the cybersecurity sector, a series of experts told EURACTIV, who highlighted that while risks will increase, avenues for defence will too.

“AI does not only open the door to new ways of cybercrime and new cyber risks, it is, together with collaboration among entities, one of the key technologies in Cybersecurity,” cyber expert Luis Búrdalo Rapa at S2 Grupo told EURACTIV.

To keep up with this fast-developing technology, cybersecurity companies will need to hire Big Data and AI experts and train their cybersecurity analysts to understand the capabilities of algorithms and prevent attacks against AI technology and attacks using AI technology, Búrdalo Rapa explained.

A technological tug-of-war

AI can potentially reduce the demand for certain entry-level jobs, where AI solutions can assist the human workforce and make the processes more efficient.

“There, the professional will then ‘work together’ with [Machine Learning] ML-supported cybersecurity solutions – in other words, an augmentation of the professional will take place,” Sven Herpig, Director for Cybersecurity
Policy at the think tank Stiftung Neue Verantwortung (SNV) told EURACTIV.

Using large-scale language models such as ChatGPT or Google Bard can simplify the entry into a very complex, theoretical subject for potential applicants.

While AI can also support further training and preparation for an entry-level job, using and developing AI-based tools requires specific knowledge and expertise in these algorithms.

While AI can be part of the solution – for example, creating opportunities for defence – it can also be part of the problem, by accelerating the number of attacks. As such, it becomes a constant source of cyber risk.

“We don't know the balance yet, namely if attacking forces will prevail over defensive ones. It will be like a tug of war, where the equilibrium point can be unchanged if the strength of the two forces grows equally,” Giuseppe D’Acquisto, Senior Technology Advisor for the Italian Data Protection Authority, told EURACTIV.

In May, the EU law enforcement agency Europol published a flash report on the potential misuse of generative AI models like ChatGPT, pointing to advanced phishing, impersonation, fake news and disinformation campaigns, and the development of new social engineering attacks and malware.

**Balancing automation and human review**

In terms of repetitive tasks and mechanical work, such as systematic pattern recognition, machines already reach higher levels of precision and have better endurance than humans.

In cybersecurity, such tasks include anomaly detection, detection of malicious behaviour patterns, and automatisation of cybersecurity alert processing.

“If we are aimed at solving simple and repetitive problems, all the tasks related to creating code for these problems can be easily automated,” D’Acquisto said.

On the other hand, algorithm-based decision-making often falls short of understanding context and explaining the rationale behind the decisions. The lack of understanding of where a decision comes from is one of the crucial reasons that make cybersecurity experts reluctant to adopt AI-based solutions in areas such as critical infrastructure.

“We use AI for both automating low complexity level tasks like, for instance, assessing the degree of potential maliciousity of a URL, so that experts can focus on higher complexity task for threat hunting or malware detection,” S2 Grupo’s Búrdalo Rapa added.

While the detection of less high-value malicious activities, for example, cybercrime, will be more likely to be partially automated, professionals will be increasingly required to acquire the skills to detect higher-value activities, research new security vulnerabilities, and assess risks.

“The work of determining whether a newly discovered vulnerability is relevant or security-critical can be strongly supported by AI technologies. New language models also have the possibility to generate code snippets and scripts,” Jonas Kernebeck, a data engineer at the software company Alpas AI, told EURACTIV.

**Future outlook**

With an eye on the future of the IT industry, experts are certain that AI will intensify and accelerate the dynamic between cybersecurity staff and hackers.

“Cybersecurity is always a race against time, new attack vectors against new defence strategies,” Kernebeck said.

While AI can help make IT systems more secure by training employees and applying attack simulations, it might also polarise the cybersecurity workforce into two classes according to their approach to this disruptive technology.

“We will have many more ‘labour class’ IT workers than today who will deal with the repetitive tasks of ‘correction’ and ‘versioning’, and very few ‘strategic’ well-paid IT workers, capable of managing the complexity of the phase of creation,” D’Acquisto said.
AI the next big challenge for the digital skills gap, EU’s Schmit says

By Luca Bertuzzi | euractiv.com

Artificial Intelligence and related fields like cybersecurity will further fuel the growing need for highly qualified talents and basic digital skills in the European Union, European Commissioner for Jobs and Social Rights, Nicolas Schmit, told EURACTIV in an interview.

The shortage of ICT experts is a widespread problem affecting most European companies, with larger companies often more in trouble in filling in the vacancies, according to data recently released from Eurostat.

For Schmit, this talent shortage is related to a multiplicity of factors, ranging from demographic trends, as Europe’s population is rapidly ageing, a mismatch between the skills acquired in education institutions and those required from the labour market, and the fact most jobs now require some sort of digital skills.

“That's the big challenge of the digital skills shortage. Hundreds of thousands of vacancies in the area of the digital economy, but also in many other companies where digital skills are also required and needed,” Schmit said.

The European Commission estimates that, in the future, up to 90% of jobs will require digital skills. Currently, one-third of Europeans lack the digital skills required in most jobs, and over 70% of companies report a lack of staff with adequate digital skills as an obstacle to investment.
The EU executive has put forth a digital skills strategy to improve the situation, striving to train more people, and offer training for re-skilling and upskilling workers, even with short-term courses of a few weeks.

The Commission is also testing a European Digital Skills Certificate with several EU countries to help people get their skills assessed and recognised by employers, trainers and public authorities across Europe.

At the same time, the world of work is being rapidly transformed by the uptake of disruptive technologies such as generative AI, Artificial Intelligence-powered models able to produce human-like content based on user input.

Asked how he thinks AI will affect the world of work, Schmit said that the picture is still to be fully defined but that his preliminary assessment is that Artificial Intelligence will mostly transform existing jobs rather than making them redundant.

"We cannot just say, let’s push AI aside. That’s too dangerous. We have certainly to create the right frameworks in which AI work functions," he explained.

"If we want to recover a strong industry in Europe, we have to use the most efficient technologies. Otherwise, we will not have the relocation of industries to Europe."

The Commissioner stressed that, to be able to use AI at its full potential, organisations will need highly qualified workers. Meanwhile, the broader workforce will also need to be trained in using AI, which can bring major productivity gains.

“What we see is a change in the role of humans in dealing with AI. A change of the qualifications, the skills you need to deal with AI," he added.

“This is the big challenge. We will have to train and educate sufficient people to handle AI. This also applies to many other issues linked to AI, like cybersecurity,” he said.

The top EU official pointed to cybersecurity as one of the fastest expanding fields, growing at the pace of thousands of jobs, as the digital transformation makes more and more sectors of the economy vulnerable to cyber-attacks – from hospitals to banks.

In this context, the Commission has recently launched a Cyber Skills Academy. On this platform, people can get informed on the kind of profiles and skills needed to become a cybersecurity expert, the learning possibilities, jobs available and qualified training providers.

“This is something which has to be permanently updated because we are not in a situation where you will be a cybersecurity expert for the next ten years. You probably need to rescale your expertise, perhaps even every six months,” Schmit said.

A key aspect of the Academy the Commissioner points to is that it includes several cybersecurity certificates that the EU recognises as meeting certain quality criteria and international standards of the field.
The European cybersecurity skills shortage is well recognized and so are the consequences. The skills shortage means that organizations of all shapes and sizes have weaker security than they should, putting themselves and everyone they interact with in harm's way.

Nanna-Louise Linde is Vice President of European Government Affairs at Microsoft.

Simply put, with a mid-sized city's worth of skilled people needed, it's time for the public and private sectors to push further and faster – together.

The recently launched EU Cybersecurity Skills Academy has the potential to make an impact on addressing the skills gap. It sets out to streamline different cyber skills initiatives and boost their overall effectiveness. That's why Microsoft pledged to support the Academy committing to train 100,000 European learners over two years. But more companies need to sign up – so far only a handful have made pledges. Imagine the possibilities when a wave of
companies gets on board – and they bring their own networks with them.

From our own efforts to build cybersecurity skills in Europe, we’ve learned that business as usual will not lead to success. Companies need to look beyond traditional recruitment and skills strategies. One option includes pivoting towards underrepresented communities, where untapped talent abounds yet opportunities are scarce. For example, MolenGeek, an innovative skilling partner and tech incubator, is based in an area of Brussels blighted by high unemployment. In partnership with MolenGeek, Microsoft provides cybersecurity training programs that lead to industry-recognized certifications. By equipping trainees with vital cybersecurity skills, the project opens new career opportunities for this historically overlooked population. In Poland, a leading cybersecurity NGO called The Kosciuszko Institute runs a cyber trainee program for Polish women and female refugees from Ukraine. And in Germany, refugees such as Arman Dinarvand who fled Iran with his family in 2018, can follow a Cybersecurity Digital Career Track at the ReDI School of Digital Integration.

Such initiatives also point at the need for companies to better support NGO skilling partners who are so essential in identifying and reaching untapped talent. It makes a huge difference when industry can help them pinpoint and analyze the skills needed by IT providers so that they build the right training programs. People want to invest their time in courses and industry-recognized certifications that will get them hired faster in better jobs. One way to address the short supply of cybersecurity trainers in projects such as ReDI School of Digital Integration in Denmark, Germany and Sweden is for volunteer trainers from the technology sector to step in. And because NGOs rarely have the transnational reach of corporates, companies can step in to help connect them with counterparts in other countries so that they can learn from each other.

Making the industry more attractive for new recruits must be part of the plan as well. A competitive hiring market needs to have a bigger and broader appeal.

First, let’s open it up. Empower and encourage women to pursue the exciting opportunities that cybersecurity offers. Show that a career in this field is about meaningful work that will literally keep the lights on, hospitals running, or planes flying. But with women representing only 25% of the global cybersecurity workforce, addressing the diversity gaps also requires intentionality in program design and execution. We must create more inclusive and supportive learning environments. That’s why it’s critical to support organizations such as Women4Cyber, a foundation working to promote and support the participation of women in cybersecurity in Europe, or WiCyS, a global community of women, allies, and advocates dedicated to advancing cybersecurity offers. Show that a career in this field is about meaningful work that will literally keep the lights on, hospitals running, or planes flying. But with women representing only 25% of the global cybersecurity workforce, addressing the diversity gaps also requires intentionality in program design and execution. We must create more inclusive and supportive learning environments. That’s why it’s critical to support organizations such as Women4Cyber, a foundation working to promote and support the participation of women in cybersecurity in Europe, or WiCyS, a global community of women, allies, and advocates dedicated to advancing women in the profession.

Second, let’s make it easier to get the right qualifications. Opportunities to learn basic digital skills will make cybersecurity qualifications more attainable. We must all accept that traditional education is not the only path. A recent OECD report “Building a Skilled Cyber Security Workforce” offers insights from five countries about the demand and supply in the cybersecurity profession over the past 10 years. The research will be extended to eleven countries, including Poland, France and Germany, next year. In England, for example, the education system offers a range of formal and informal cybersecurity training pathways. Some non-formal training options, such as bootcamps, present shorter, flexible learning avenues that end with potential job opportunities. These intensive courses lower access barriers to entry level roles and are also a valuable stepping stone for those seeking to specialize within the cybersecurity sector.

Third, let’s ensure that qualifications can travel. Cross border recognition of qualifications will make the industry more attractive, more diverse and more agile. For example, Edukamu is a Finland-based tech skills online platform with English language learning. It now offers a micro-degree in cybersecurity. Its beauty is that the credits earned in the micro-degree can be counted towards other university cybersecurity degrees in any EU country. An approach we need to make the norm, not the exception.

Cybersecurity Skills Academy, on-the-ground partnerships with NGOs and broader collaboration amongst industry that we will create a resilient, skilled cybersecurity workforce that will secure our digital future.