OECD Skills Studies

Building a Skilled Cyber Security Workforce in Europe

INSIGHTS FROM FRANCE, GERMANY AND POLAND

OECD

OECD Skills Studies

Building a Skilled Cyber Security Workforce in Europe

INSIGHTS FROM FRANCE, GERMANY AND POLAND

OECD
BETTER POLICIES FOR BETTER LIVES

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of the Member countries of the OECD.

This document, as well as any data and map included herein, are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Please cite this publication as:
OECD (2024), *Building a Skilled Cyber Security Workforce in Europe: Insights from France, Germany and Poland*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/3673cd60-en.

ISBN 978-92-64-92964-7 (print)
ISBN 978-92-64-47876-3 (pdf)
ISBN 978-92-64-48994-3 (HTML)
ISBN 978-92-64-87273-8 (epub)

OECD Skills Studies
ISSN 2307-8723 (print)
ISSN 2307-8731 (online)

Photo credits: Cover © vs148/Shutterstock.com.

Corrigenda to OECD publications may be found on line at: www.oecd.org/about/publishing/corrigenda.htm.

© OECD 2024

The use of this work, whether digital or print, is governed by the Terms and Conditions to be found at https://www.oecd.org/termsandconditions.

Foreword

Governments, businesses, and individuals worldwide continue to face significant threats from cyber security breaches. The demand for cyber security professionals has grown substantially in recent years, and this trend is expected to continue, resulting in labour shortages in several countries. The first step in addressing the scarcity of skilled workers in the cyber security sector is to understand the supply and demand dynamics of cyber security skills. Governments and organisations can utilise this information to pinpoint vulnerabilities and determine areas requiring additional resources. From the demand side, analysing job postings can help identify trends in demand for cyber security professionals and the skills needed to strengthen organisations' cyber security. Simultaneously, studying cyber security education and training programs offers insights into the evolving development of the cyber security workforce, shedding light on potential mismatches between supply and demand.

This report analyses the demand for cyber security professionals in France, Germany and Poland and zooms in on the provision of cyber security education and training programs in France. The report aims to provide a comparative analysis of cyber security demand in France, Germany and Poland, with a detailed analysis of the education and training programmes and policies put in place in France to make the profession more attractive and diverse. The report is the third in a series of studies that aim to expand knowledge on the cyber security workforce and related education and training provision in various regions and countries.

This work has been carried out by the OECD Directorate for Employment, Labour and Social Affairs and the OECD Centre for Skills. The report was prepared by Diego Eslava and Annikka Lemmens (Chapter 1 and 2) and Iván Bornacelly and Viktoria Kis (Chapter 1 and 3), under the supervision of Fabio Manca, Malgorzata Kuczera, and Marieke Vandeweyer. Editorial assistance was provided by Jennifer Cannon. Valuable comments were given by Mark Pearson (OECD Deputy Director for Employment, Labour and Social Affairs) and El Iza Mohamedou (Head of the OECD Centre for Skills), as well as by colleagues from the OECD Directorate for Science, Technology and Innovation.

The OECD is grateful to stakeholders in France for their input and feedback throughout the project, in particular the Ministry of National Education and Youth, Ministry of Digital Transformation and Cyber Campus, as well as the multiple training providers and universities that participated throughout the consultations. Our warm thanks go to the ministries in the countries analysed that provided feedback to the report and to the many education and training institutions, businesses, research institutions, and other organisations who generously shared their knowledge and insights during bilateral discussions. The support from Microsoft Philanthropies is highly appreciated.

Table of contents

FIGURES

TABLES

Follow OECD Publications on:

https://twitter.com/OECD

https://www.facebook.com/theOECD

https://www.linkedin.com/company/organisation-eco-cooperation-development-organisation-cooperation-developpement-eco/

https://www.youtube.com/user/OECDiLibrary

https://www.oecd.org/newsletters/

Executive summary

The digital transformation has heightened the need to implement effective cyber security measures across all European countries. The increasing reliance on digital technologies, accelerated by the rapid adoption of remote work in response to the COVID-19 pandemic, necessitates a strategic focus on cyber security and the development of a skilled workforce capable of addressing potential threats. Despite employment levels in cyber security being at an all-time high, analyses of the field show that there is still a substantial workforce gap, with Europe alone facing a shortage of over 300 000 professionals.

This report analyses the evolution of the demand for cyber security professionals using recent data from millions of online job postings (OJPs) collected in France, Germany and Poland for the period between January 2018 and June 2023. The demand for cyber security professionals is experiencing an increasing trend across all three countries. Notably, growth rates of job postings published on line for cyber security surpass the average growth of other occupations. In Poland, in particular, the demand for cyber security professionals stands out for its rapid post-February 2020 growth, surging three times faster than that for other occupations. The analysis delves into employers' demands, by looking at the most frequently requested characteristics in candidates for a cyber security role. The study reveals that firms look for candidates with tertiary education, a trend consistent across France, Germany, and Poland. In France, for instance, candidates with a master's degree are often preferred, while in Germany and Poland, a bachelor's degree or equivalent is more common in the demands of employers. Notably, in France, about 28.1% of job postings with explicit education requirements seek candidates with short-cycle tertiary education, specifically a "brevet de technicien supérieur" (BTS) or the pre-2020 "diplôme universitaire de technologie" (DUT). Interestingly, 30% to 35% of job postings do not specify educational qualifications, indicating an increasing emphasis on experience and informal education as indicators of cyber security competence.

Key skills sought in cyber security professionals include programming proficiency and familiarity with various software and digital tools across all three countries examined in the report. In Germany and France, knowledge of ICT security legislation, standards, and information security strategy skills are highly valued. Similarly, transversal skills such as conceptual thinking, spreadsheet expertise, and business process understanding are typically in high demand, whereas in Poland, there is a notable focus on project management and public speaking skills. The analysis also indicates that the demand for cyber security skills advertised in online job postings has become more specialised in between 2019 and 2022, being concentrated in a narrow set of technical and cyber occupations in France and Germany.

The report also explores the available supply of training opportunities in cyber security, zooming in on the landscape of education and training programmes in France and the policies and strategies to enhance the accessibility and relevance of these programmes. The study shows that, in France, cyber security education and training is multifaceted, ranging from courses focusing on basic awareness for the general public to advanced technical training for specialised roles. The focus of this study is on the learning opportunities for entry-level positions provided by formal and non-formal training programmes. The formal education supply is diverse including programmes at different levels of education such as vocational and technological baccalaureates, short-cycle tertiary programmes (e.g. Brevet de Technicien Supérieur, BTS), and academic and professional bachelor's level (e.g. Bachelors universitaires de technologie, BUT). Advanced degrees in this field are particularly relevant in France, including engineering programmes and specialised master's degrees, reflecting the high demand for highly skilled cyber security professionals. The programmes responding to this demand include both programmes that specifically focus on cyber security and programmes with a slightly broader focus, which include cyber security in their curriculum or as an area of specialisation (e.g. system engineering, information security, information systems management, ethical hacking, network security and information auditing).

France provides a wide array of non-formal cyber security training for young people and adults, distinct for its practical focus and shorter duration. Offered by a diverse mix of private companies, industry associations, and online platforms, these programmes can last from a few weeks to months, leading to highly-valued certifications. They cover foundational and advanced cyber security topics, aligning with industry standards and certifications. Notable examples include the Continuing Education Programmes (*Formation continue*) and Certificate Training (*Formation certifiante*), designed for professionals enhancing their skills or transitioning into cyber security. France offers many courses on line, which broadens access to foundational and specialised training.

Multiple policies and initiatives have been implemented to reduce cyber security skill gap. Industry involvement in the programme delivery has been crucial in providing work-based learning opportunities in the sector. Apprenticeships have enhanced graduates' employability by establishing strong connections with specific companies and industries, often resulting in immediate permanent job placements. Similarly, employers' close connection with training providers has been key in bringing cyber security professionals into the teaching workforce. Regulations have permitted and encouraged experienced professionals to enter the teaching profession, either as contractual or substitute teachers, without needing a national examination, providing a flexible solution to address fluctuations in demand and challenges arising from tenured teacher shortages.

Diversifying cyber security education and training programmes is key to addressing the growing demand for skilled professionals in this rapidly evolving field in France. Emphasis can be placed on diversifying enrolment, particularly by increasing female participation. Strategies range from ensuring job postings, including those in cyber security, are gender-inclusive, to implementing national campaigns to break down role stereotypes in the field. Additionally, the availability of a wide range of formal and non-formal education options in cyber security contributes to providing training opportunities that can cater to the diverse needs of learners and the industry. France is enhancing socio-economic diversity in cyber security through higher education programmes like BTS, BUT, and professional bachelor's degrees, with quotas and progression routes for vocational or technological baccalaureate graduates, particularly in pathways like "networks and telecommunications."

1 Key insights for building a skilled cyber security workforce in Europe

This chapter provides an overview of the report’s objectives and rationale and summarises the main takeaways. It discusses the results from the analyses of the demand for cyber security professionals in France, Germany and Poland. It also summarises the main findings from the analysis of the landscape of cyber security education and training programmes in France. It concludes with actionable policy pointers.

Cyber security skills in a rapidly evolving digital world

Cyber security breaches are a significant threat to governments, businesses, and individuals worldwide. As economies transition towards increased use of digital and online technologies, cyber risks are often greater than can be managed by traditional approaches to data security. The spectrum of dangers has expanded, ranging from disruptions in the supply chain to sophisticated ransomware attacks. In addition, responses to the COVID-19 pandemic have accelerated society's dependence on digital technology, especially through the rapid adoption of remote work to sustain operational continuity for businesses, schools, and various services during lockdowns. However, the extensive embrace of remote work has exposed individuals and organisations to unparalleled cyber security threats (World Economic Forum, 2022[1]). As a substantial portion of the workforce now operates remotely or adopts hybrid work models, cybercriminals gain heightened opportunities to exploit vulnerabilities in digital security measures. Similarly, the advent of artificial intelligence (AI) in cyber security has transformed the threat landscape, leading to more sophisticated and adaptive cyber threats, which may impact the skill content of training programmes and national cyber skills policies. Governments around the world are aware of the heightened risk, and the European countries which are focus of this report (France, Germany and Poland) all have national strategies and policies to improve their nations' cyber security (Box 1.1).

A workforce shortage compounds these cyber security challenges. While the cyber security workforce has reached an all-time high, with an estimated 5.5 million professionals already employed, a global shortage of 3.9 million workers is still estimated in this field ((ISC)2, 2023[2]). According to an assessment from the International Information System Security Certification Consortium (ISC)² (2023[2]) Europe faces a deficit of over 347 000 cyber security professionals. In France for instance, a shortage of nearly 60 000 cyber security experts was estimated in 2023. According to these estimates, France, together with Ireland are the only European countries with a decrease in the cyber security workforce gap year over year[1] ((ISC)2, 2023[2]). Additionally, the demand for professionals in sectors which are relevant for the cyber security sector (e.g. digital, engineering and maths-related occupations) has increased recently in France, Germany and Poland (see Chapter 2). This increase signals the impact of digital innovation, digital sector expansion and the increase of digital hubs, which will all lead to a broader need for cyber security professional across multiple sectors.

Within individual countries and specific sectors, the lack of cyber security professionals can be even more pronounced due to intense competition for the limited number of employees. This often results in certain sectors, such as governments and central banks, struggling to attract highly skilled security professionals compared to other sectors, like the finance industry, which can offer more financially rewarding employment opportunities (ENISA, 2021[3]). Additionally, organisations such as ENISA (the European Union Agency for Cyber Security) have issued warnings regarding the shortage of cyber security skills in the broader labour market, not just a lack of cyber security professionals (ENISA, 2021[3]), which also highlights the increasing demand of professionals with updated knowledge on broader areas such as cyber security legal and policy frameworks (ENISA, 2023[4]). Effective training in cyber security at all levels is key to overcome both the shortages of professionals and the limited knowledge of cyber security of the general population.

In addition to the points mentioned above, the current cyber security workforce faces a significant diversity challenge. Women constitute only 24% of the global cyber security workforce ((ISC)2, 2022[5]). This figure is even lower in France (17%), partly due to the small proportion of women trained in the information and communication technology (ICT) field overall. Among OECD countries, some like Israel (53%), Norway (31%), Canada (28%), and Sweden (27%) have a higher percentage of women among ICT graduates. The representation remains low at the bachelor's level; for instance, in France in 2021, women made up just 17% of ICT graduates (see Chapter 3). This underrepresentation not only reduces the available talent pool for key roles in cyber security but also limits diversity in thought and perspective (Grau-Sarabia and Fuster-Morell, 2021[6]), which are vital for tackling complex cyber threats and challenges. Therefore, it is crucial to focus on attracting, recruiting and retaining more women in the field, as this will help access a broader talent pool and address the shortage of skilled professionals in the industry.

Collaborative initiatives between the private and public sectors can contribute to equip the cyber security workforce with rapidly evolving skills. Some initiatives are already underway, notably through developing cyber security ecosystems (i.e. network of entities and technologies collaboratively enhancing digital security and resilience against cyber threats). An example is the French Cyber Campus, which serves as a hub for cyber security expertise and collaboration, bring together businesses, government entities, academia, and research institutions to tackle cyber security challenges. In partnership with the National Information Systems Security Agency (Agence nationale de la sécurité des systèmes d'information, ANSSI). Similarly, governments within the European Union (EU) have developed a common skills framework and regional strategies to address the cyber security skills shortage (ENISA, 2023[7]). These initiatives, including the French Cyber Security Strategy, align with broader European efforts such as Horizon Europe and the Digital Europe Programme, aiming to establish a unified cyber security skillset across the EU (European Commission, 2023[8]). In terms of co-ordination of existing initiatives in the EU, in 2023, the EU Cyber Security Skill Academy launched the Cyber Skills Academy, a co-ordinated approach to boost the EU cyber security workforce and address the cyber security talent gap in the region (EC, 2023[9]). Similarly, the European Cyber Security Competence Centre and Network (ECCC), Europe’s new framework to support innovation and industrial policy in cyber security, is an ecosystem aimed at increasing the capacities of the cyber security technology community, shielding the economy and society from cyberattacks, maintaining research excellence, and reinforcing the competitiveness of the EU industry in this field (ECCC, 2024[10]).

Box 1.1. Cyber security national strategies and cyber security skills frameworks

The speed of digital innovation and proliferation of cyber threats have pushed the French, German and Polish governments to develop national cyber security strategies (NCSs) to overcome these fast-evolving cyber security challenges. The governments intend to economically stimulate the cyber security sector, strengthen the cyber security workforce, increase the development of cyber security solutions within their own countries, and strengthen the governments resilience against cyber threats. The French Government, for instance, has allocated EUR 1 billion to help boost the cyber security sector as part of the “France 2030” initiative, with EUR 720 million stemming from public funding (French government, 2023[11]).

Both Germany and Poland have integrated the national strategy for cyber security with their most recent broader national security strategies (Government of Poland, 2020[12]; Federal government of Germany, 2023[13]). These integrated strategies are about security in all its facets, one of which is security in cyber space. The goals of the Polish strategy include enhancing resilience against cyber threats, strengthening defensive capabilities and improving information protection in public, military, and private sectors. The German strategy aims to actively modernise the governments cyber security infrastructure and enhance its capabilities in order to defend Germany against cyberattacks.

This report: Understanding the demand for and the supply of cyber security skills in a set of countries

What this report is about

Understanding the supply and demand dynamics in the cyber security labour market is crucial to tackle skill shortages. This understanding helps organisations and governments pinpoint critical weaknesses and allocate resources effectively. One way of looking into the demand for labour is by utilising online job postings (OJPs). These offer valuable insights into demand trends and key skills needed for a secure cyber environment, while analysis of cyber security education and training programmes sheds light on workforce development in this sector.

This report represents the third major output of an extensive project aimed at deepening the understanding of the cyber security workforce and the corresponding education and training provision across multiple regions and countries (see Box 1.2). Each report of this project, including the current one, is divided into two parts. The first analyses the demand for cyber security professionals leveraging the information contained in OJPs. The second examines the supply side: the landscape of cyber security education and training programmes. In particular:

- The analysis of the demand for cyber security professionals in the labour market leverages big data intelligence to identify trends in employers' demands through an examination of both the volume and content of these new postings published online by firms seeking to hire cyber security workers. The current report focuses on the demand for cyber security professionals in three European countries: France, Germany and Poland.
- The analysis of the supply of training options in cyber security takes a deep dive into the policies and strategies implemented to broaden and diversify the cyber security workforce. Each report delves into a single case study country for this supply-side analysis. This report focuses on France.

Box 1.2. The "Building a skilled cyber security workforce" project

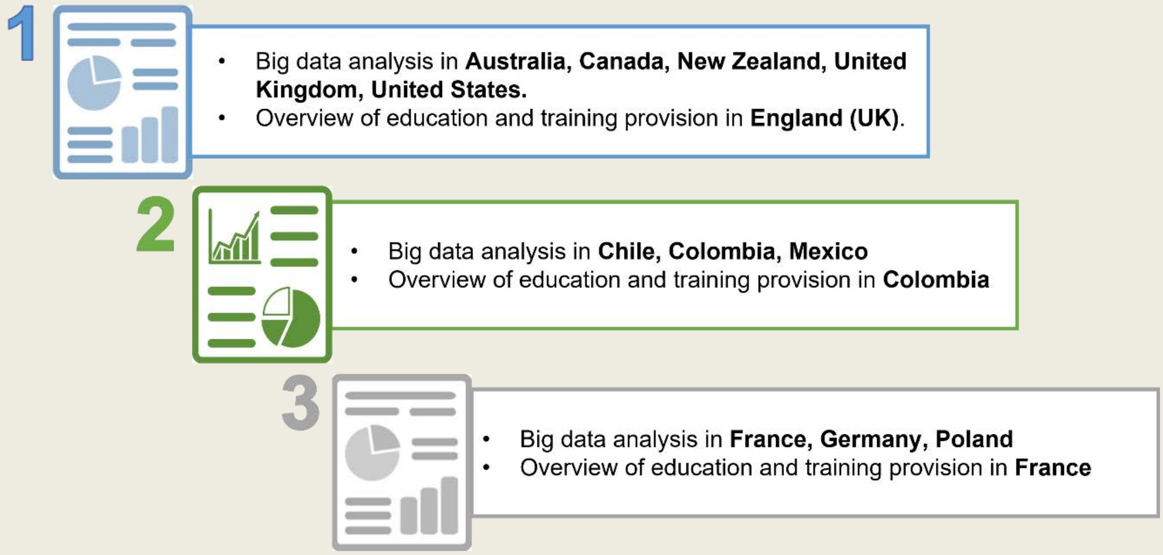
The rationale of the project

As the demand for cyber security professionals' soars globally, labour market shortages are emerging. This project aims to provide policymakers and businesses with timely, detailed insights into the demand and supply of cyber security skills, drawing from global best practices. It leverages OECD's expertise to identify key roles and skills in global markets for a secure digital infrastructure. The initiative also reviews how various national education systems develop these skills and promotes a forum for discussing best practices and future skill needs in cyber security.

The structure of the project

The project is segmented into three components that blend big data intelligence with policy analysis to examine the demand and supply of cyber security skills, as well as the policies and strategies in place to grow and diversify the cyber security workforce, thereby addressing cyber security skill deficits. Each of these three parts zeroes in on a different group of countries (see Figure 1.1), investigating three to five countries for the demand-side analysis and a single country for an in-depth case study on the supply side. This is the third OECD report of three segments that will be synthesised for these analyses. The first report was published in March and the second in September of 2023 (OECD, 2023[14]; OECD, 2023[15]).

Figure 1.1. Outputs of the cyber security project



- Big data analysis in **Australia, Canada, New Zealand, United Kingdom, United States.**
- Overview of education and training provision in **England (UK)**.

- Big data analysis in **Chile, Colombia, Mexico**
- Overview of education and training provision in **Colombia**

- Big data analysis in **France, Germany, Poland**
- Overview of education and training provision in **France**

Methodology

Using big data to understand cyber security skills demand in three countries

The analysis of big data, and in particular the study of the information contained in OJPs have become instrumental in tracking labour market developments, playing a pivotal role in providing insights into job demand and industry trends (OECD, 2022[16]; OECD, 2023[17]). Increasingly, research on labour market dynamics relies on real-time big data to better capture recent trends and gain insights at a more granular level than what would be possible with more traditional labour market data. In order to conduct a timely and comprehensive analysis of the demand for cyber security professionals, this report utilises data extracted from nearly 82 million online job advertisements sourced from three selected countries: France, Germany, and Poland.

Specifically, this report examines trends in the demand for cyber security professionals between January 2018 and June 2023. Employing text mining and Natural Language Processing (NLP) techniques, the report classifies cyber security job postings and extracts key information used to analyse job requirements, including desired roles and skills and makes it possible to gain insights into evolving employer needs. The aim is to monitor labour market dynamics, identify trends, and inform tailored policies and training programmes to meet the evolving demands of the European cyber security labour market.

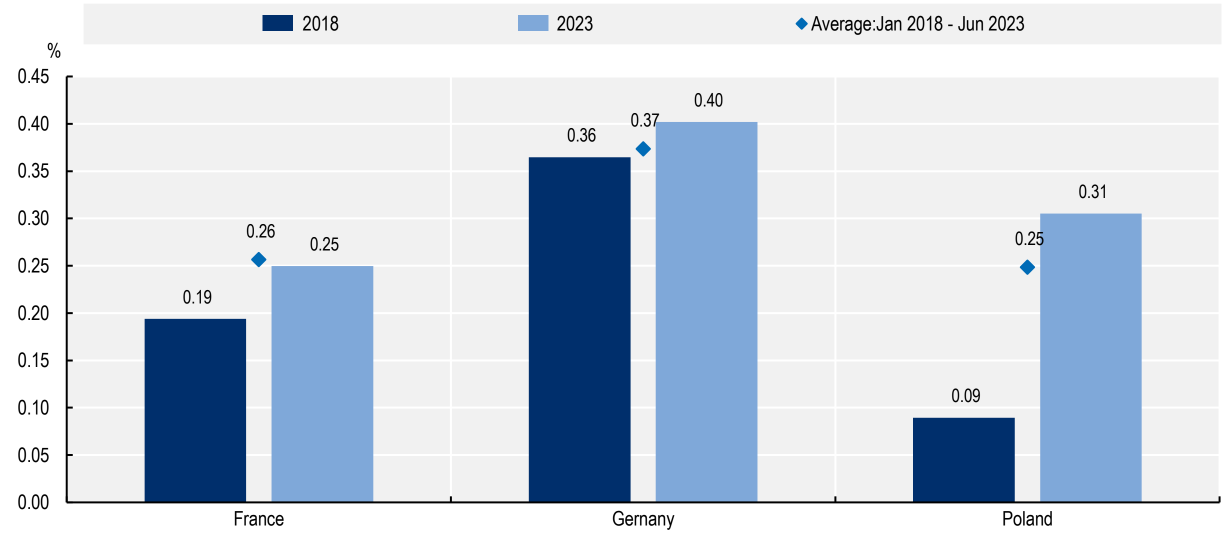
A case study to zoom in on strategies for cyber security education and training provision

The report also focuses on the availability of education and training options in the cyber security field in France. Notably, the approaches to cyber security education and training programmes in France exhibit a diverse range of designs, reflecting the unique needs and policies of the country. This report aims to provide insights into how France can develop, deliver, and promote education and training for cyber security roles. It presents a comprehensive case study of the French system, detailing programmes, policies, and initiatives that could inspire other countries developing their cyber security education sectors. The French approach includes formal education programmes at undergraduate levels and below (e.g. professional baccalaureate and advanced technician qualification, BTS) and non-formal training such as continuing education programmes and certificate training. This report also looks into advanced qualifications in cyber security, such as a master's degree, since employers consider them highly important for cyber security roles. Additionally, it reviews strategies for expanding the cyber security workforce in France, particularly those facilitating access for newcomers. The analysis is based on national data, literature and interviews with key stakeholders in the French education and cyber security sectors.

The demand for cyber security professionals is on the rise in France, Germany and Poland

The demand for cyber security professionals is experiencing a robust and increasing trend across all three countries, especially in the period after the peak of the COVID-19 pandemic. Notably, growth rates for cyber security OJPs surpass those for other occupations. In Poland, in particular, the demand for cyber security professionals stands out for its rapid post-February 2020 growth, surging three times as fast as the average for other occupations. Cyber security-related OJPs in France and Germany experienced growth rates 40-30% higher, respectively, than those for other professions. This accelerated growth has led to an increased share of cyber security job postings compared to the total number of OJPs in the three countries analysed in the report. Specifically, Figure 1.2 shows that cyber security OJPs accounted for, in average, 0.32% of all OJPs advertised in 2023, a significant increase compared to the same share in 2018 (0.22%). While the demand for cyber security professionals is strong in the three countries, the faster growth experienced in Poland signals that relatively smaller markets for cyber security professionals have tended to grow faster compared to more developed markets, such as Germany, suggesting a rapid expansion of cyber security demand across countries.

Figure 1.2. Share: Cyber security posts as a percentage of total online job postings



Source: OECD calculations based on Lightcast data.

Results also highlight the varied demand for different types of cyber security professionals. Across the countries analysed, the core of the demand is for cyber security architects and engineers, who account for 38% to 45% of total cyber security OJPs from January 2018 to June 2023. These professionals are responsible for designing and modelling security solutions. Other cyber security-related roles are important and represent a significant share of the demand. Cyber security auditors and advisors (who offer guidance on the efficiency and compliance of security solutions) accounted for 17.4% of the overall demand in Germany, a figure significantly higher than in Poland and France.

However, the demand for different roles within the cyber security profession has shifted in the last few years, a fact that underscores that the cyber security job market is evolving, reflecting the adoption of new technologies and priorities by firms. For example, both France and Germany have seen an increase in the demand for cyber security analysts, individuals providing insights to support planning, operations, and maintenance of systems security.

The majority of cyber security OJPs are concentrated in the main cities in France, Germany, and Poland, where key enterprises and government hubs are located. Notably, 61% of cyber security OJPs in these countries are located in metropolitan areas. This share is 1.7 times higher compared to the proportion of all OJPs located in cities (36%). This trend underscores a significant concentration of cyber security roles in metropolitan settings, influenced by industries like finance, technology, and professional services, which typically thrive in metropolitan settings due to the availability of skilled talent, robust infrastructure, and market demand.

An analysis of enterprises' requirements mentioned in OJPs shows that a typical candidate for a cyber security job needs a tertiary education. This result is consistent across the three countries analysed. In France, employers more often prefer candidates with a master's degree, whereas a bachelor's or equivalent is more commonly sought after in Germany and Poland. Additionally, a significant portion of job postings in France (28.1% of those with explicit education requirements) specifically asks for short-cycle tertiary education leading to degrees known as "*brevet de technicien supérieur*" (BTS) or before 2020, the "*diplôme universitaire de technologie*" (DUT). Beyond formal requirements, approximately 30% to 35% of job postings do not explicitly mention education requirements (see Chapter 2), potentially suggesting an emphasis on experience and informal education as signals of cyber security skills, rather than a strict reliance on formal degrees.

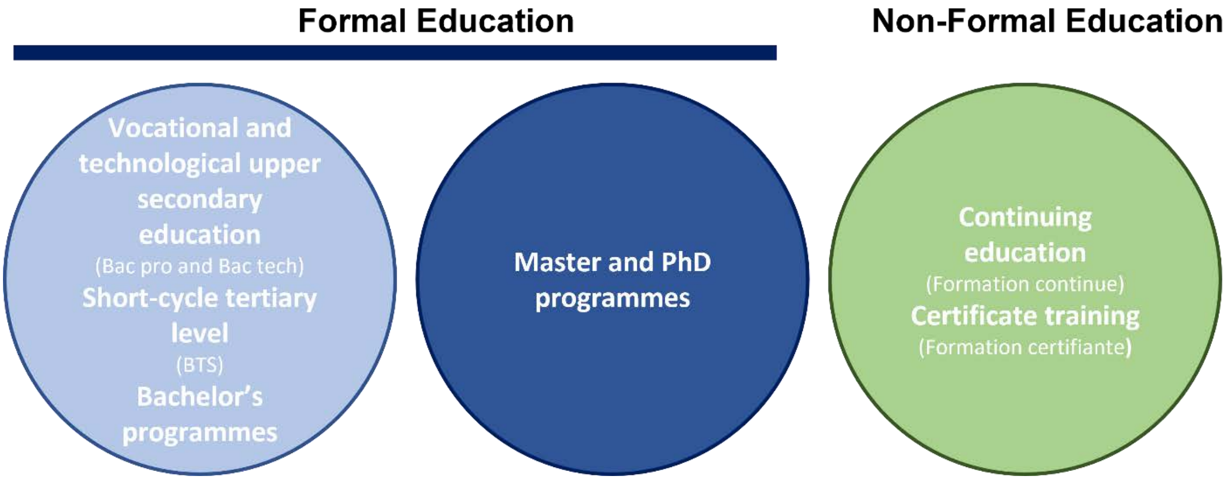
Regarding the most highly sought after skills for cyber security professionals, proficiency in programming and familiarity with various software and digital tools are crucial across the three examined countries. Furthermore, skills such as knowledge of ICT security legislation and standards, and information security strategy skills rank among the most in-demand in Germany and France.[2] Shifting the focus to professional skills, employers who sought to hire cyber security professionals in France and Germany prioritise conceptual thinking, expertise in spreadsheets, and a grasp of business processes, while in Poland there is a distinct emphasis on project management and public speaking.

An examination of the demand for cyber security skills among all OJPs reveals a trend towards the cyber-related skill demands becoming increasingly specialised in between 2019 and 2022. In other words, the mentions of cyber-related skills in OJPs have tended to concentrate in a narrower set of cyber and technical occupations in France and Germany, pointing to the profession becoming more specialised. In Poland, possibly due to the very large surge in demand, cyber security skills (in particular the mention of "cyber security" in OJPs) has permeated a larger number of different job postings as the market was expanding in terms of its complexity and roles demanded by firms.

The provision of cyber security education and training programmes in France is diverse

The case study for France illustrates that there are diverse educational and training pathways leading to cyber security roles, offering opportunities for progression (see Figure 1.3). Formal cyber security education programmes is accessible at various levels, encompassing upper secondary education (mainly through vocational and technological baccalaureate), short-cycle tertiary programme, and higher education. Notably, enrolment in cyber security programmes has been increasing, particularly in higher education, especially in bachelor's programmes *(License),* reflecting the labour market requirements (see Chapter 2). Basic cyber security skills are also being integrated into upper secondary education, including in Vocational and Technological Baccalaureate courses. These courses span a range of professional and technological fields, focusing on ICT topics. Education and training opportunities in this field also encompass work-based learning programmes, such as apprenticeships in cyber security at various educational levels, enabling learners to develop practical skills on the job.

Figure 1.3. Cyber security education and training programmes take many forms in France



Note: Formal education, which leads to formal qualifications such as advanced technician qualifications (Brevet de technician supérieur, or BTS), includes courses and programmes offered by universities, technological, professional and technical institutions. For this study, programmes at the master's level and above are excluded from the analysis. Non-formal education and training include courses outside the formal education system and not leading to formal qualifications (but awarding certificates in some cases), such as certificate training.

Complementing these formal cyber security qualifications, young people and adults in France can also participate in non-formal training. This type of training is usually shorter and more flexible than programmes in the formal education system. They may lead to certificates but do not confer formal qualifications. Various organisations offer professional certificates or qualifications, providing targeted instruction and practical experience. The recent surge in demand for specialised ICT skills, such as cyber security, has led to a significant expansion in other forms of short courses, like specialised training modules available through continuing education. In 2021, approximately 40 400 institutional certificates were awarded, which is nearly double the number from 2010, when just over 24 000 were offered. Learners can also engage with certificate training programmes that provide streamlined, practical training culminating in industry-recognised credentials (e.g. ISO 27001 Lead Auditor or Certification-ISO27001 in Cyber Security Fundamentals) which are also highly required by employers (see Chapter 2). Additionally, multiple online courses contribute to the non-formal training landscape in the digital field. In the realm of cyber security, nearly 10 100 courses were available on France's most popular e-learning platforms (see Chapter 3). These courses offer flexible and accessible learning opportunities, enabling individuals to acquire expertise quickly and efficiently, and in some cases at no cost.

The cyber security skill gap is being addressed through multiple policies and initiatives (see Chapter 3). Industry involvement in the programme delivery has been crucial in providing work-based learning opportunities in the sector. Apprenticeships have enhanced graduates' employability by establishing strong connections with specific companies and industries, often resulting in immediate permanent job placements. Similarly, employers' close connection with training providers has been key in bringing cyber security professionals into the teaching workforce. Regulations have permitted and encouraged experienced professionals to enter the teaching profession, either as contractual or substitute teachers, without needing a national examination, providing a flexible solution to address fluctuations in demand and challenges arising from tenured teacher shortages.

In France, expanding and diversifying cyber security education and training programmes is key to addressing the growing demand for skilled professionals in this rapidly evolving field. Emphasis is placed on diversifying enrolment, particularly by increasing female participation. Strategies range from ensuring job postings, including those in cyber security, are gender-inclusive, to implementing national campaigns to break down role stereotypes in the field. Additionally, the availability of a wide range of formal and non-formal education options in cyber security contributes to providing training opportunities that can cater to the diverse needs of learners and the industry.

Multiple initiatives have been implemented to increase the socio-economic diversity within the cyber security profession. Higher education programmes offered by University Institutes of Technology, including BTS, BUT, and professional bachelor's programmes, play a significant role in diversifying the social backgrounds of future cyber security professionals. For example, progression routes for graduates of vocational or technological baccalaureates have been established, with quotas facilitating these transitions to some disadvantage students. In BTS programmes, the quota varies, but typically around two-thirds of entrants are graduates of vocational and technological baccalaureates. For BUT programmes, half of the places are reserved for graduates of a related technological baccalaureate. Specifically, in cyber security, a pathway exists for graduates of the "Sciences and Technologies of Industry and Sustainable Development" technological baccalaureate to progress into a BUT programme in "Networks and Telecommunications."

Policy pointers for building a skilled cyber security workforce

The insights derived from the analysis of the demand for cyber security professionals in France, Germany and Poland and the detailed analysis of the cyber security education and training in France underscore diverse opportunities for these countries to tackle labour and skills shortages in the sector.

Providing structured and comprehensive information on cyber security roles and skills

- The cyber security profession is constantly evolving, based on the evolution of cyber risk. This also changes employers' needs, which creates a challenge for individuals seeking to enter the cyber security labour market for and training institutes who want to create new training programmes in understanding demands for certain cyber security roles and skill requirements. Collaboration is needed across employers, educators, governments and learners to create a structured and comprehensive characterisation of the cyber security profession to reduce shortages in the cyber security labour market. Current initiatives to monitor indicators of the evolution of cyber security labour markets exist, providing insights on the supply of cyber security professionals. ENISA, in co-operation with the EU Commission, has made progress in developing indicators to track progress in EU Member States to increase the number of cyber security professionals (EU Monitor, 2023[18]).
- Enhancing collaboration among stakeholders in the cyber security sector is crucial for effective skills anticipation (OECD, 2016[19]). France, for instance, has invested heavily in skills anticipation in multiple sectors, by establishing a centralised platform for data sharing and analysis, involving public authorities, chambers of commerce, sector organisations, and educational institutions, which can streamline the process (CEDEFOP, 2023[20]). This centralisation reduces fragmentation and improves the accuracy of identifying current and future skill requirements. Additionally, developing standardised methodologies for skills assessment and updating training programmes accordingly will ensure that the workforce remains equipped to address evolving cyber security challenges. Such a co-ordinated approach will facilitate more efficient allocation of resources and better prepare workforces for the demands of the cyber security sector.
- Raising employers' awareness, especially among SMEs, about the significance of a skilled cyber security workforce in mitigating cyber risks is crucial. Adherence to cyber security frameworks and standards is key, as it offers essential guidance, best practices, and a common language for both organisations and professionals. The European Cyber Security Skill Framework (ECFS), that was launched in 2022, is a practical choice, providing a unified understanding of the necessary roles, competencies, skills, and knowledge in cyber security. It facilitates the recognition of cyber security skills and supports the design of related training programmes. Utilising a shared framework enables countries to develop comprehensive cyber security strategies, provide a better understanding of

common ground of cyber security roles within and beyond the profession, and improve the provision of training and education.

- Governments can aim to promote cyber security as a viable and exciting career path, by providing educational resources, showcasing a variety of roles within the sector, and engaging students in interactive learning experiences. This can for instance be done by using initiatives such as The Tomorrow Cyber Specialist (*DemainSpécialisteCyber*) developed by the Ministry of Education and Youth (MENJ), which seeks to break down stereotypes and encourage more people to enter the cyber security profession, thereby helping to secure France's digital future.

Giving visibility to cyber security education and training programmes

- Integrating cyber security technical skills into digital-related training programmes can enhance cyber security awareness and skills across all digital sector professions. Initiatives such as CyberEdu, an ANSSI label to signal education programmes that integrate cyber security elements, expand cyber security skills into a broader spectrum of educational offerings, including vocational, technological and general baccalaureate programmes and work-based learning opportunities.
- Clear pathways for graduates from cyber security programmes (e.g. CyberEdu-certificated programme) to either enter the labour market or advance to higher qualifications, such as professional bachelor's programme, or obtain industry-recognised certifications, will enhance their employability and provide opportunities for more in-depth cyber security training.
- Signalling high-quality education and training is key in cyber security. High-quality labels like SecNumedu benefit institutions by attracting learners and boosting prestige, while ensuring learners receive up-to-date, in-depth training. Holding a SecNumedu-accredited certificate enhances employment prospects in the competitive cyber security industry, valued by employers seeking qualified candidates.

Boosting employer participation in the design and delivery of cyber security programmes

- Integrating work-based learning like internships and apprenticeships into cyber security education programmes effectively links industry and academia. This not only arms graduates with relevant skills but often leads to job placements. Strong partnerships between educational institutions and employers across sectors are essential to create diverse, practical learning environments.
- Enhancing cyber security education quality can be achieved by integrating experienced industry professionals into the teaching workforce. This requires relaxing regulatory requirements to allow these professionals to serve as contractual or substitute teachers without traditional examination processes. Tertiary education programmes commonly use industry experts as part-time teachers alongside full-time teacher-researchers, reflecting this approach's effectiveness.
- Joint applied research projects and flexible teaching models, pairing full-time academics with industry professionals, enhance cyber security education by blending theory with practice. Leveraging initiatives like Campus Cyber for knowledge exchange ensures educational programmes stay current with industry developments. This approach keeps teaching content and methodologies updated in line with the rapidly evolving cyber security sector.

Diversifying the profile of cyber security professionals

- Offering flexible learning schedules is essential for diverse cyber security education pathways. Institutions should implement hybrid models blending online and in-person teaching, tailored to both traditional and apprentice learners. This adaptable approach ensures an inclusive, efficient environment for all students pursuing cyber security careers.

- Enhancing quotas and transition programme in technology-focused universities and engineering schools for vocational or technological baccalaureate graduates promotes student diversity. This strategy includes reserving places for these graduates, especially high achievers, and offering support like bridging programme and mentorships. It diversifies the socio-economic mix in advanced cyber security education and improves student success in rigorous academic settings.
- Boosting socio-economic diversity in cyber security can be achieved by expanding vocational and technological baccalaureates among disadvantaged students. This involves increasing funding, developing cyber security-focused curricula, and promoting these paths in underprivileged communities. Strengthening the link to higher education in cyber security and lowering access barriers to the profession will also facilitate a smoother transition for these students into the workforce.
- Targeted educational and professional development initiatives are crucial for expanding gender diversity in the cyber security profession. Expanding mentorship programmes, where experienced female cyber security professionals guide and support young women, is key. Such mentorship should encompass career planning, skill development, and networking opportunities.

Box 1.3 highlights interesting practices put in place in France aimed at expanding and diversifying the cyber security workforce.

Box 1.3. Relevant practices from France

France has implemented multiple initiatives and strategies to expand and diversify its cyber security workforce. Efforts focus on improving coordination between the industry and training providers, enhancing the responsiveness of educational programmes, and facilitating their provision. Strategies also aim to improve the image of cyber security roles and increase interest in the sector, particularly among women and young people. Key practices include:

- **Les cadettes de la cyber** (Les Cadettes de la Cyber, 2021[21]): Launched by the Cyber Excellence Centre, this programme fosters young women's careers in cyber security through mentorship, training in cyber geopolitics, managerial skills, and public speaking. It facilitates job transitions with internships, job dating sessions, and personalised coaching, and empowers cadettes to be ambassadors at events and on social media.
- **Campus Cyber** (Campus cyber, 2023[22]) A national initiative serving as a hub for cyber security expertise, it brings together businesses, government, academia, and research to address cyber security challenges. It focuses on fostering innovation, knowledge exchange, and addressing the shortage of qualified educators through partnerships and scalable training solutions.
- The **French National Acceleration Strategy for Cyber security** (Gouvernement, 2021[23]), Supported by significant investment, this strategy aims to enhance cyber defences and digital security. Goals include increasing the cyber sector's turnover, doubling jobs, supporting cyber security unicorns, and promoting cyber security culture and research. Educational integration at all levels and public awareness campaigns are central to this strategy.
- Higher education institutions have expanded **apprenticeship opportunities in cyber security**, offering practical experience alongside academic learning. Businesses value apprentices for fresh perspectives and building a tailored talent pipeline, with varied candidate profiles influenced by educational backgrounds and recruitment cycles.
- The **SecNumedu** label, awarded by the **French National Agency for the Security of Information Systems (ANSSI)**, identifies high-quality specialised programmes in cyber security, meeting rigorous training standards. It enhances the prestige of educational institutions

and guarantees students a quality education, improving employment prospects. The label concerns engineering and master's programmes and some professional bachelor's degrees.

- **"TomorrowCyberSpecialist"** (*DemainSpécialisteCyber*) (MENJ, 2023[24]), launched in 2023 by ANSSI, MENJ, and Campus Cyber, is a French national campaign to address the cyber security skill gap. Aimed at middle, high school, and post-secondary students, it seeks to raise cyber security awareness and highlight career diversity in the field, encouraging interest among young girls and boys. This initiative is part of a broader effort to familiarise students with various professions.
- The **CyberEdu label** (CyberEdu, 2023[25]), established by ANSSI, marks education programmes in France that integrate cyber security. This initiative, following the 2013 Defense and National Security White Paper, aims to weave cyber security awareness into all digital-related training. CyberEdu certifies various programmes, from vocational baccalaureates to short-cycle tertiary qualifications, focusing on cyber security competencies.

References

(ISC)2 (2023), *2023 Cybersecurity Workforce Study*, https://www.isc2.org/Research (accessed on 15 January 2024). [2]

(ISC)2 (2022), *2022 Cybersecurity Workforce Study*, https://www.isc2.org/Research (accessed on 15 January 2024). [5]

Campus cyber (2023), *concept: Réunir les acteurs de la sécurité numérique au sein d'un lieu totem pour protéger la société et faire rayonner l'excellence française du domaine*, https://campuscyber.fr/. [22]

CEDEFOP (2023), *Skills anticipation in France*, https://www.cedefop.europa.eu/en/data-insights/skills-anticipation-france#group-details. [20]

CyberEdu (2023), *Le projet*, https://www.cyberedu.fr/pages/le-projet/. [25]

EC (2023), *Cybersecurity Skills Academy: a coordinated approach to boost the EU cyber workforce*, https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy. [9]

ECCC (2024), *European Cybersecurity Competence Centre and Network - About us*, https://cybersecurity-centre.europa.eu/about-us_en. [10]

ENISA (2023), *Communication on the Cybersecurity Skills Academy*, https://digital-strategy.ec.europa.eu/en/library/communication-cybersecurity-skills-academy. [4]

ENISA (2023), *European Cybersecurity Skills Framework (ECSF)*, https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework. [7]

ENISA (2021), *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/ (accessed on September 2023). [3]

EU Monitor (2023), *Closing the cybersecurity talent gap to boost the EU's competitiveness, growth and resilience ('The Cybersecurity Skills Academy')*, https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vm2dme2qmizc. [18]

European Commission (2023), *Shaping Europe's digital future*, https://digital-strategy.ec.europa.eu/en/activities/digital-programme. [8]

Federal government of Germany (2023), *Robust. Resilient. Sustainable. Integrated Security for Germany - National Security Strategy*, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (accessed on November 2023). [13]

French government (2023), *Communique de Presse - France 2030 | Le Gouvernement lance une nouvelle vague de l'appel à projets pour*, https://www.economie.gouv.fr/files/files/2023/communique_AAP_cybersecurite.pdf (accessed on November 2023). [11]

Gouvernement (2021), *Un plan à 1 milliard d'euros pour renforcer la cybersécurité*, https://www.gouvernement.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite. [23]

Government of Poland (2020), *National Security Strategy of the Republic of Poland 2020*, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf (accessed on November 2023). [12]

Grau-Sarabia, M. and M. Fuster-Morell (2021), "Gender approaches in the study of the digital economy: a systematic literature review", *Humanities and Social Sciences Communications*, Vol. 8/1, https://doi.org/10.1057/s41599-021-00875-x. [6]

Les Cadettes de la Cyber (2021), *Les Cadettes de la Cyber est un programme du Pôle d'Excellence Cyber (PEC)*, https://les-cadettes-de-la-cyber.org/qui-sommes-nous/. [21]

MENJ (2023), *Lancement de la campagne nationale "DemainSpécialisteCyber" pour faire découvrir la cybersécurité et ses métiers*, https://www.education.gouv.fr/lancement-de-la-campagne-nationale-demainspecialistecyber-pour-faire-decouvrir-la-cybersecurite-et-379968. [24]

OECD (2023), *Big Data Intelligence on Skills Demand and Training in Umbria*, OECD Publishing, Paris, https://doi.org/10.1787/4bbbbfd6-en. [17]

OECD (2023), *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. [14]

OECD (2023), *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/9400ab5c-en. [15]

OECD (2022), *Skills for the Digital Transition: Assessing Recent Trends Using Big Data*, OECD Publishing, Paris, https://doi.org/10.1787/38c36777-en. [16]

OECD (2016), *Getting Skills Right: Assessing and Anticipating Changing Skill Needs*, Getting Skills Right, OECD Publishing, Paris, https://doi.org/10.1787/9789264252073-en. [19]

World Economic Forum (2022), *Global Cybersecurity Outlook 2022*, https://www.weforum.org/reports/global-cybersecurity-outlook-2022/. [1]

Notes

[1] Among six European countries for which the cyber security workforce gap was estimated (France, Germany, Ireland, Netherlands, Spain and United Kingdom).

[2] This partially reflects the decision to include keywords that are associated with the EU’s General Data Protection Regulation as part of the classification of cyber security skills, given the importance of this regulation in this geographical area.

2 The demand for cyber security professionals in Europe

This chapter provides an analysis of millions of online job postings that describe the demand for cyber security professionals in France, Germany and Poland between January 2018 and June 2023. The chapter compares the demand for cyber security professionals with its context by investigating the demand for digital, engineering, and maths-related occupations. The chapter analyses the demand for four different cyber security roles, and the geographical location of the demand. Moreover, the research highlights education requirements and specific skills that are in high demand within the cyber security professions, as well as the demand for cyber security skills throughout the labour market.

Introduction

In Europe, as in other parts of the world, the reliance on digital technologies within organisations has surged, underlining the critical importance of robust cyber security measures. Increased interconnectedness and use of digital technologies do not only bring economic advantages but are accompanied by heightened cyber risk. This susceptibility necessitates a strategic focus on cyber security, demanding a proficient workforce which is capable of identifying, analysing, and responding to potential threats.

Within this context, there is increasing evidence of a shortage of trained workers in the cyber security sector across the world. According to estimates from (ISC)² (2023[1]) there exists a deficit of over 347 000 cyber security professionals throughout Europe. In France for instance, a shortage of nearly 60 000 cyber security experts was reported in 2023. This news prompted the then-director of the French cyber security agency (ANSSI) to identify "this *human resources* challenge as the most significant constraint for the future of cyber security in France" (Pollet, 2022[2]). Additionally, organisations such as ENISA (the European Union Agency for Cybersecurity) have issued warnings regarding the shortage of cyber security skills in the broader labour market, not just a shortage of cyber security professionals (ENISA, 2021[3]).

Effectively tracking the evolution of cyber security labour demand and skill requirements is critical to be able to address current and future shortages. To accomplish this objective, timely and detailed information is necessary to shed light on the evolving skill demands in the rapidly changing cyber security landscape. Different data sources can provide valuable insights into the skills required in the cyber security sector. Traditional data sources such as labour force surveys or national accounting data are able to provide information on how many people are working in a certain profession and the contribution of a certain sector to GDP. Using online job postings (OJPs) as a data source offers numerous advantages over traditional methods *(*Box 2.1*).* OJPs provide a timely means to track the emergence of skill demands, given their daily collection from online job listings. Additionally, they offer exceptionally detailed insights into the specific technologies and skills that are in high demand within the cyber security field. However, it is worth noting that OJPs may not comprehensively cover all occupations and sectors, particularly those not typically advertised on line, as highlighted *by OECD* (2021[4]) *and* Cammeraat and Squicciarini (2021[5]). These limitations, however, are likely to be small in the current study as this investigates a specific part of the labour market demand that is typically channelled through OJPs.

This chapter monitors the evolution of the demand for cyber security professionals from January 2018 to June 2023 in three European countries: France, Germany, and Poland. It leverages the information contained around 80 million OJPs collected from the Internet by Lightcast*.*[1] The remainder of this chapter is divided into two sections. The first section describes the context in which digital occupations are developing and afterwards examines the demand for cyber security professionals over the past five years, as measured by OJPs. This section also includes an overview of the demand for different types of cyber security roles and an analysis of where the demand is located. The second section delves into the education and skills that are demanded from cyber security professionals in the three European countries under examination, using information collected from the job descriptions provided by employers within job postings. Box 2.1 includes some methodological notes useful for interpreting the results.

Box 2.1. Methodological note: Interpreting the results from online job postings (OJPs)

The wealth of information contained in job postings can offer a very detailed overview of the demand of enterprises for cyber security profiles. This box summarises the main methodological approaches used to leverage these data and improve the readability of the results and insights shown below. Annex 2.A and the footnotes of each figure provide additional details.

Using OJPs to identify the recent evolution of demand

- **Cyber security OJPs:** Data from Lightcast for European countries do not explicitly include a “cyber security occupation title”. Instead, each individual job posting collected from the Internet is mapped to broader occupational groups using the International Standard Classification of Occupations (ISCO-08). This occupational taxonomy is, however, too aggregated to identify cyber security professionals specifically. To precisely identify cyber security job postings between January 2018 and June 2023, this report uses a text mining approach that matches key expressions that appear in the job titles of each online job posting. Annex 2.A provides more details on the keywords used to identify a job posting as cyber security-related.
- **Cyber security roles:** Using the job titles available in OJPs, this chapter disaggregates data into job roles and tracks the demand for each. Four specific roles were chosen in accordance with the two earlier reports in the “Building a skilled cyber security workforce” project (OECD, 2023[6]; OECD, 2023[7]) Annex Table 2.A.2 contains the comprehensive list of keywords associated with each role.
- **Groups of digital, engineering and maths-related occupations:** The analysis provides insights on 25 digital, engineering and maths-related occupations used as benchmarks to compare the trends in their demand with the demand for cyber security professionals. The 25 occupations were classified into five occupational groups: 1) Computer and data analysts/administrators; 2) Software developers and programmers; 3) ICT technicians; 4) Maths-related professions; and 5) Engineers and technicians.

Using information from OJPs to infer skill demands in the cyber security profession

- **Skill bundles**: Using Natural Language Processing (NLP) methods, the analysis in this chapter identifies the most relevant technical and professional/transversal skills in employer demands cyber security positions collected through OJPs in France, Germany and Poland (more details can be found in Annex 2.A). Technical skills refer to “*specialised skills, knowledge or know-how needed to perform specific duties or tasks*” (UNESCO - UNEVOC, 2023[8]), while professional/transversal skills are those “*not specifically related to a particular job, task, academic discipline or area of knowledge and that can be used in a wide variety of situations and work settings*”.
- **Skills relevance**: As detailed in Annex 2.A the “skill relevance” index should be interpreted as a measure of the relevance of a given skill for the cyber security profession. The closer the value assigned to a certain skill is to one, the higher the relevance of the skill for the occupation.

It is also important to note that some of the keywords collected do not represent skills *strictu sensu.* Some of them, for instance, are technologies or tools (i.e. Python or Microsoft Azure), while others identify knowledge areas (i.e. Network or Information Security). For the sake of simplicity, this study pools all keywords together under the term “skills” and only differentiates between them if necessary.

The demand for cyber security professionals in recent years

The impact that the digital transition has on labour markets has garnered significant attention in recent years. A recent study by the OECD (2022[9]), for instance, highlighted the substantial increase in demand for digital professionals across various labour markets, underscoring the rapid integration of digital technologies in workplaces across diverse sectors and occupations. Global trends such as the digital transition and the creation of new technologies do not only propel the demand for cyber security professionals, but also affect the demand for related (digital) occupations. Employers are increasingly adopting cloud computing, artificial intelligence and making more use of data. While these developments lead to opportunities for economic growth, on the one hand, they also lead to more potential cyber security threats, which necessitates a skilled cyber security workforce.

Among the many digital occupations experiencing demand growth, cyber security professionals have stood out for the most rapid growth (OECD, 2023[6]; OECD, 2023[10]). By contrast, the demand for most digital, engineering and maths-related occupations have experienced a slower but more steady growth over time. In many cases, the development and integration of new technologies across sectors are accompanied by a more pressing need for cyber security personnel. For instance, the healthcare sector in France has been actively undergoing digital transformation efforts to improve patient care, streamline operations, and enhance efficiency. This transformation has involved various aspects, including the adoption of electronic health records (L'espace numérique de santé and le dossier médical partagé), telemedicine, and connected medical devices (CNIL, 2022[11]). Large projects like adopting electronic health records require professionals across different occupations to integrate digital solutions, from programmers, data analysts, and lawyers to cyber security experts.

Describing the context: The digital transition and its impact on the labour market

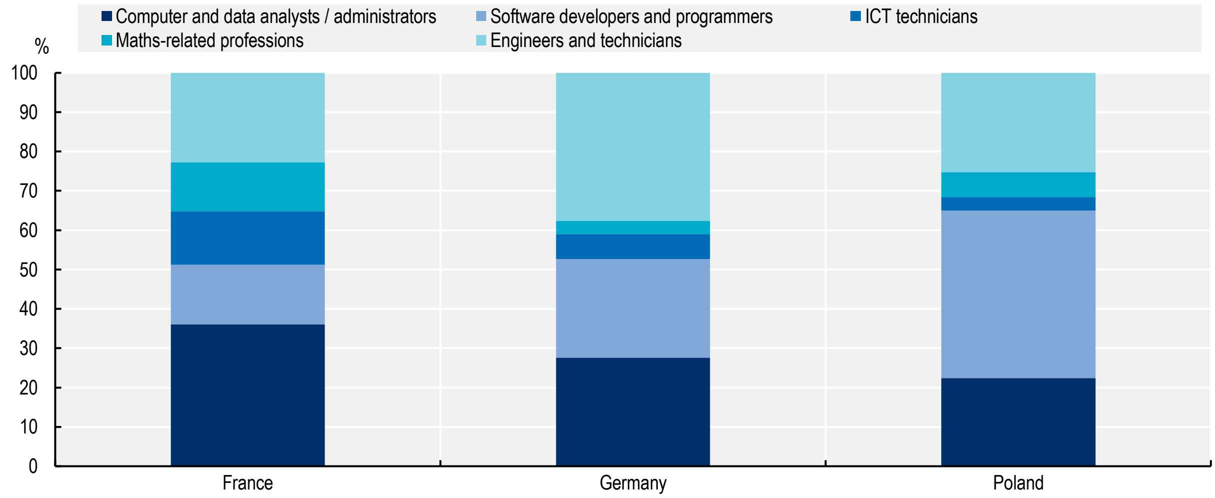
Over recent years, the increasing reliance on technology and digital platforms in various sectors has fundamentally reshaped the nature of work and the skills that are in demand. As businesses and industries have integrated more digital tools and practices into their operations, there has been a surge in the need for professionals with digital expertise. These digital professionals encompass a wide range of roles – from software developers to data analysts. This section describes the context within which the demand for cyber security professionals has emerged, by looking into how digitalisation has impacted the labour market and pushed the demand for digital, engineering and maths-related professionals more broadly across countries. These types of professionals often operate in sectors which experience a relatively high cyber risk.

Results in this section focus on the demand for digital, engineering and maths-related roles by looking into the trend demand of 25 occupations, classified into five occupational groups. The choice of these occupational groups is based on the methodology used in (OECD, 2023[10]), and includes these five occupational groups: 1) Computer and data analysts/administrators; 2) Software developers and programmers; 3) ICT technicians 4) Maths-related professions; and 5) Engineers and technicians.[2]

> *What has been the trend demand for digital, engineering and maths-related jobs in recent years?*

The average share of OJPs for digital, engineering and maths-related jobs compared to all OJPs from January 2018 – July 2023 is 6.4% in France, 14.3% in Germany, and 11.7% in Poland.[3] A notable observation is the variance in the leading occupational group across the three nations, as determined by the volume of OJPs. In France, computer and data analysts/administrators represent 36.1% of the digital, engineering, and maths-related OJPs. Meanwhile, in Germany, engineers and technicians lead with 37.7% of OJPs. In contrast, Poland sees the highest demand for software developers and programmers, accounting for 42.6% of OJPs (Figure 2.1).

Figure 2.1. Composition of digital, engineering and maths-related occupations



Source: OECD calculations based on Lightcast data.

The demand for computer and data analysts/administrators in France is linked to a particularly strong demand for systems analysts (ISCO 2511) and systems administrators (ISCO 2522). These two roles not only rank among the most highly demanded occupations but have also exhibited significant growth in the average number of OJPs per month in between January 2018 – February 2020 compared to March 2020 – June 2023. For instance, the demand for systems analysts nearly tripled, while that for systems administrators increased by 2.5 times. Additionally, data show a larger demand for both ICT technicians (13.6% of all digital, engineer and maths-related OJPs) and for maths-related jobs (12.5%) in France than in the other two countries. The share for ICT technicians is around twice as large compared to Germany, and four times as large as in Poland (Figure 2.1).

Both system administrators and ICT user support technicians are part of the information technology (IT) support ecosystem and contribute to ensuring that an organisation's IT systems and services function effectively. Information communication technology (ICT) user support technicians are primarily responsible for providing technical assistance and support directly to end-users (ISCO-08). A high demand for these types of jobs can indicate that the use of digital technologies is becoming more integrated in France, which can also lead to an increased demand for cyber security professionals.

The share for maths-related jobs in France is 3.8 times larger than in Germany and nearly twice as large as that in Poland. Financial and investment advisers are the most highly sought-after maths-related role within France. For instance, on average there were around 4 706 OJPs looking to hire people for this role per month in between March 2020 and June 2023. Financial and investment advisers are tasked with developing financial plans for individuals and organisations and managing funds on their behalf (ISCO-08). The finance sector uses sensitive data, and financial institutions are often the target of cyberattacks. Moreover, the financial sector is becoming increasingly reliant on (big) data, heightening the need for cyber security specialists to achieve adequate data protection.

In Germany a significant volume of digital, engineering and maths-related OJPs is allocated to engineers and technicians, accounting for 37.7% of these OJPs compared to 22.8% in France and 25.2% in Poland. The engineering sector has historically been of key importance within the German economy with, for instance, 1.1 million employees working in mechanical engineering in 2021 and a total revenue of EUR 2 096 billion in the manufacturing industry in 2020 (German Federal Foreign Office, 2023[12]). Germany's industrial landscape is currently undergoing a significant digital transformation, with companies increasingly relying on automation, digital technologies, and artificial intelligence to drive their operations (German Federal Foreign Office, 2023[12]). Companies in the different Germany industry sectors put an emphasis on innovation, with for instance investments of EUR 26 billion in the automotive industry, EUR 9 billion in the electrical industry, EUR 7.2 billion in mechanical engineering, and EUR 5.5 billion in the pharmaceutical industry and ICT in 2021 (Stifterverband, 2023[13]). A digital transformation can lead to increased cyber risks, which in turn increases the importance of having skilled cyber security personnel.

As can be seen from Figure 2.1, the share of OJPs for software developers and programmers is the largest in Poland. This share closely resembles what was observed in Chile and Mexico during the years 2021 and 2022 (OECD, 2023[10]). In Poland, France, and Germany, software developer positions account for 28%, 12%, and 20% of all digital, engineering, and maths-related OJPs, respectively. The relatively high demand for software developers in Poland is in part due to Poland being a highly sought-after "nearshoring" destination in Europe. Nearshoring involves outsourcing specific business operations to a neighbouring country with lower labour costs. While similar to offshoring, enterprises that make use of nearshoring specifically select nearby countries for these operations. Another reason for the high demand is that Poland holds a prominent position in the software development industry within Central Eastern Europe. Approximately 25% of the developer population in this region is located in Poland, constituting roughly 300 000 professional developers spread across various technology hubs within the country (CBI, 2022[14]). The prevalence of OJPs for software developer roles suggests a growing digitalisation in the Polish job market. As digitalisation advances, the likelihood of cyber threats rises, necessitating the development of a skilled cyber security workforce to address these emerging challenges.

How has the demand for cyber security personnel evolved across countries?

Within the context of increased use of digital technologies and data, the need to have specialised cyber security personnel has grown as well. The cyber security profession encompasses a wide variety of different roles and jobs. Most cyber security professionals are in charge of securing data, systems, infrastructure and other cyber resources from failures, hazards and cyber threats that affect an organisation's mission and operation (World Economic Forum, 2022[15]). This section focuses on tracking the demand for these professionals in France, Germany and Poland in between January 2018 and June 2023, using the information contained in OJPs. As mentioned, this report uses text mining techniques, by matching the text contained in job titles to certain expressions that are indicative of the cyber security sector, to determine which OJPs are looking for cyber security personnel (more details can be found in Annex 2.A).[4]

In recent years, many European countries have experienced a notable surge in the demand for cyber security professionals, something that is echoed across other regions of the world as well. For instance, (OECD, 2023[6]) shows that especially after 2020, the demand for cyber security professionals increased significantly in countries such as the United States, Canada, the United Kingdom or Australia and New Zealand. Another recent study, (OECD, 2023[10]) shows a strong increase in the demand for cyber security professionals in three Latin American countries in between 2021 and 2022.

Analysis carried out in this report for France, Germany and Poland also illustrates a pattern of increasing demand for cyber security experts from January 2018 to June 2023. Table 2.1 also underscores that the growth of the number of average monthly OJPs for cyber security professionals outpaced that of other occupations in all three countries, especially when comparing the pre-COVID period (January 2018 – February 2020) to the time after February 2020. This result likely reflects the expansion of remote working activities around the world, which imposed new technological challenges for enterprises that faced increased cyber security risk. Poland, in particular, stands out for having experienced a rapid growth after February 2020, with the demand for cyber security professionals having increased three times as fast as that for other occupations. Cyber OJPS in France and Germany, by contrast, saw 1.4 and 1.3 times the growth of other professions (Table 2.1).

Table 2.1. Average monthly OJPs pre-covid, during and post-covid

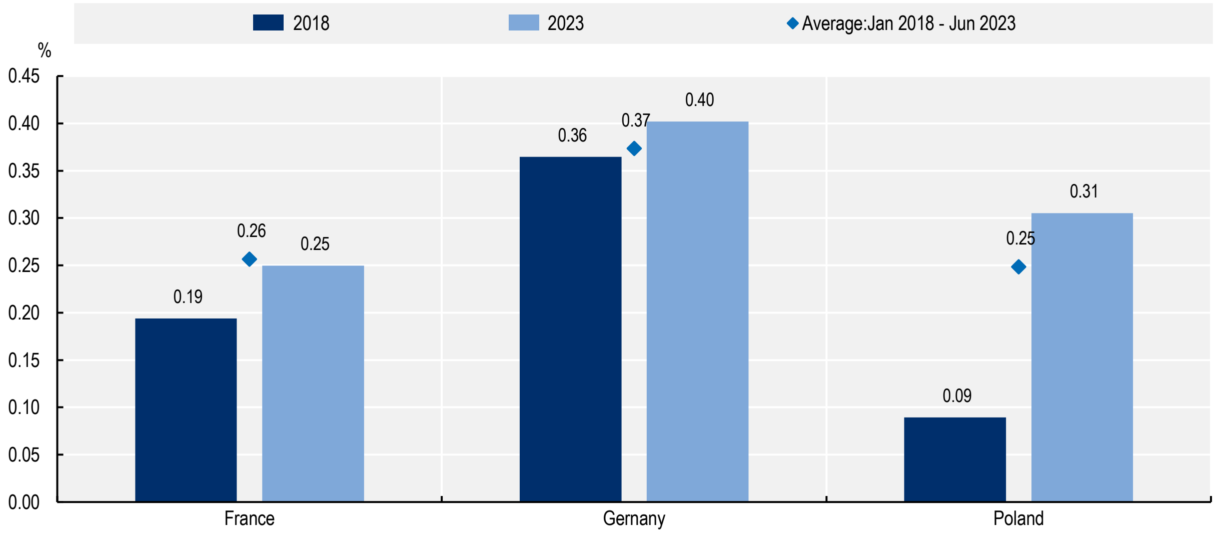
Country	Job type	Average monthly OJPs Jan 2018 – Feb 2020	Average monthly OJPS Mar 2020 – Jun 2023	Growth rate between the two periods
France	Cyber	477.9	1 965.4	311%
	Non-Cyber	221 883.9	708 984.3	220%
Germany	Cyber	1 907.4	2 752.6	44%
	Non-Cyber	535 117.1	713 500.6	33%
Poland	Cyber	38.4	402.7	948%
	Non-Cyber	27 367.3	116 705.2	326%

Source: OECD calculations based on Lightcast data.

Figure 1.2 provides insights regarding the size of the labour market for cyber security professionals. In 2018, job postings seeking cyber security professionals in Germany represented 0.36% of the total job postings. Notably, this figure was nearly twice as high as the share of postings in France and six times greater than that in Poland at that time. This suggests that Germany had already established a more developed cyber security labour market compared to the other two European countries by 2018. By 2023, the share of German cyber security job postings had increased to 0.4%, putting it on par with the figures seen in the United Kingdom in 2022 (OECD, 2023[6]).

Poland started with a smaller share of 0.09%, comparable to the overall share of cyber security job postings in New Zealand between January 2012 and June 2022 (OECD, 2023[6]). However, this share nearly tripled due to the substantial growth in the number of Polish cyber security job postings compared to other professions, placing it in between the levels observed in France and Germany. The shares of cyber OJPs in France and Poland in 2023 were similar to those of Australia and Canada in 2022 (OECD, 2023[6]).

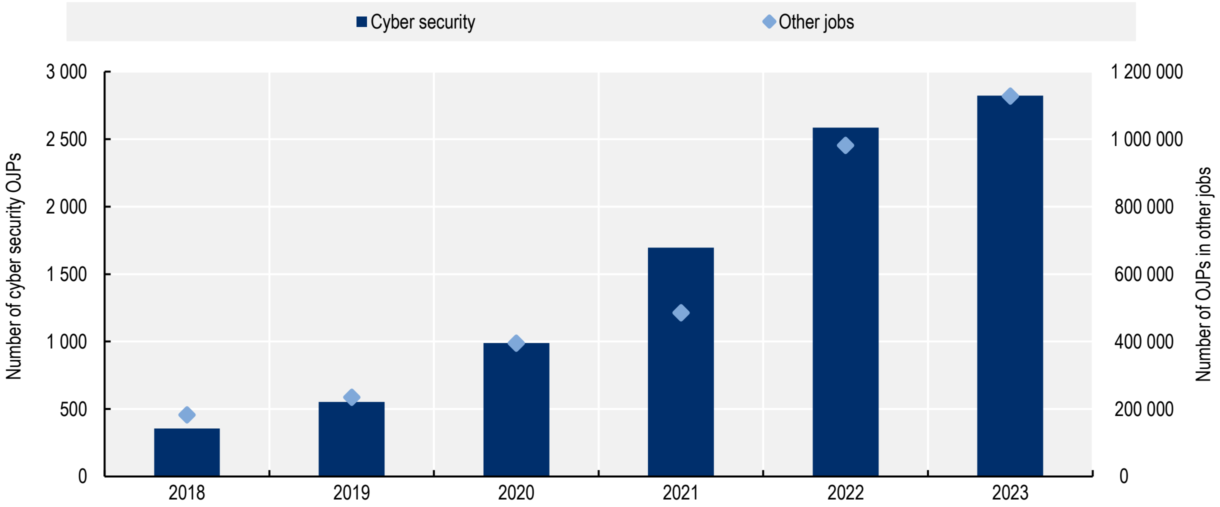
Figure 2.2. Cyber security posts as a percentage of total online job postings (OJPs)



Source: OECD calculations based on Lightcast data.

Zooming in at the country level, the number of OJPs for cyber security professionals in France saw a stronger growth than that for non-cyber jobs in between 2018 and 2023, especially during and after the Covid-19 pandemic (Table 2.1).[5] France faced labour shortages for high-skilled labour between 2020 and 2021 (OECD, 2021[16]), which is likely to have influenced the proliferation of job postings published on line, encompassing both cyber and non-cyber roles.[6]

Figure 2.3. Average monthly (cyber security) job postings in France



Source: OECD calculations based on Lightcast data.

When examining the dynamics of cyber security job postings in France, it becomes evident that specific factors underlie the rapid growth in this field, which has also been stronger than in the average labour market. To start with, the French Government has prioritised the cyber security sector for years, through various national strategies, plans, and investments but has invested even more strongly into this industry in 2021, 2022 and 2023. examples. (See Box 2.2 for more details about France's national strategy.)

Furthermore, the country witnessed a significant surge in teleworking due to the pandemic, with large shares of French employees continuing to work remotely into 2021 and beyond. For instance, 27% of employees worked remotely in January 2021, compared to 4% in 2019, and 80% of these teleworkers said to want to continue working remotely in the future (Dares, 2022[17]). In 2022, as well, 38% of employees worked from home at least some of the time, and employees' and employers' attitudes towards working from home were mostly positive (République Française, 2023[18]). Increased use of working from home elevates the necessity for cyber security measures.

Box 2.2. Policy initiatives and cyber security strategy in France

The French Government has pursued the development of a strong cyber security policy for nearly two decades, with the first national strategy dating back to 2008 (ANSSI, 2011[19]). The latest strategy for the acceleration of cyber security has been published as part of the overarching "France 2030" initiative. The French Government has allocated EUR 1 billion for this purpose, with EUR 720 million stemming from public funding (French government, 2022[20]). The economic objective of this acceleration strategy is to triple the revenue generated within the cyber security sector by 2025. Furthermore, this strategy aims to foster the development of cyber security solutions with France itself, and to strengthen the links and synergies between stakeholders in the sector. Moreover, this strategy strives to promote the widespread adoption of cyber security solutions by individuals, businesses, communities, and the state, by for instance starting the international Forum for Cyber Security. Lastly, it aims to train more young people and professionals to be able to work in cyber security professions, by for example adapting educational programmes at every level to better meet the cyber security needs expressed by the labour market (French government, 2022[20]).

To realise these objectives, the government has made a number of investments in 2021, 2022 and 2023. For instance, it established the Campus Cyber (further details available in Box 2.5). In addition, the government launched the Cybersecurity Research Programme (PEPR), which received EUR 65 million from the "France 2030" plan and is dedicated to the advancement of French cyber security sector (French government, 2023[21]). Notably, in June 2022, the programme started two new research initiatives: one of which will study attacks on digital systems (such as smartphones and connected objects), while the other will study the robustness of cryptographic systems. A forthcoming wave of projects is anticipated in 2024, as applicants were invited to submit their proposals until the 7 November 2023 (French government, 2023[22]).

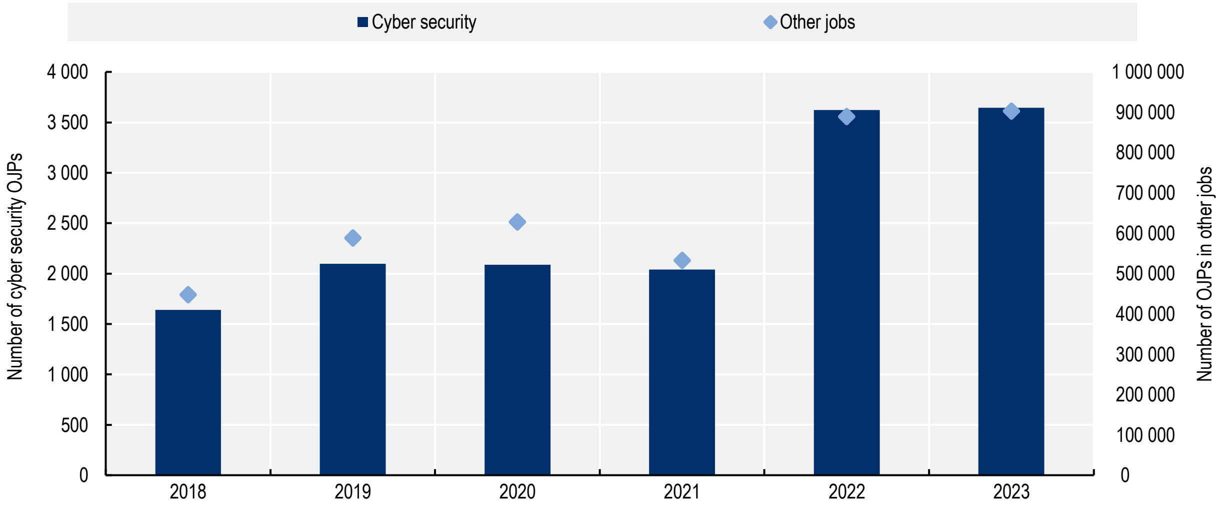
Unlike France and Poland, Germany experienced a more moderate increase in the average monthly number of OJPs for both cyber security and non-cyber security positions when comparing the periods before and after February 2020 (Table 2.1). The relatively slower growth of cyber security OJPs in Germany can be attributed, in part, to the size of the German cyber security market at the beginning of the period analysed, 2018, compared to that in the other countries under study. Similar to what was found in (OECD, 2023[6]) for the United States, a slower rate of growth in the demand for cyber security professionals may reflect an already more mature German cyber security labour market in which growth has perhaps started to slow down. Nonetheless, it is also important to notice that the German Government has had a strong focus on cyber security for years, with its first national cyber security strategy implemented in 2011, which was updated in 2016 and 2021 (CCDCOE, 2020[23]; Federal Ministry of the Interior and Community, 2021[24]). (See Box 2.3 for more information on the most recent German cyber security strategy).

Box 2.3. Germany's national cyber security strategy

Germany's most recent cyber security strategy, released in 2021 (Federal government of Germany, 2021[25]) encompasses four key areas: society, private industry, government, and EU/international affairs. The strategy specifically emphasises the transformation of the Federal Office for Information Security into a central hub for federal and state co-operation in cyber-crime prevention. Moreover, the strategy aims to fortify digital sovereignty, ensuring a safe digital transformation of Germany. This involves reinforcing Germany's digital economy through targeted backing of technologies and collaboration with relevant researchers.

However, as of June 2023, the government has incorporated cyber security into the National Security Strategy, integrating it with security initiatives across various domains (Federal government of Germany, 2023[26]). The National Security Strategy underscores the collective responsibility of the state, businesses, research sectors, and society at large to bolster cyber security. The Federal Government intends to actively develop its cyber security architecture and enhance its capabilities in order to defend Germany against cyber-attacks. This will be achieved by, for instance, transforming the Federal Office for Information Security into a more autonomous and centralised information security hub, expanding the German Cyber agency, and improving the government's ways of identifying aggressive cyber activities early on (e.g. by increasing capacities for data analysis, making available several independent IT infrastructures, among other strategies). The strategy also mentions that research will continue to focus on the cyber security aspects of technological revolutions, including artificial intelligence, quantum computing, quantum cryptography, and speech recognition.

Figure 2.4. Average monthly (cyber security) job postings in Germany

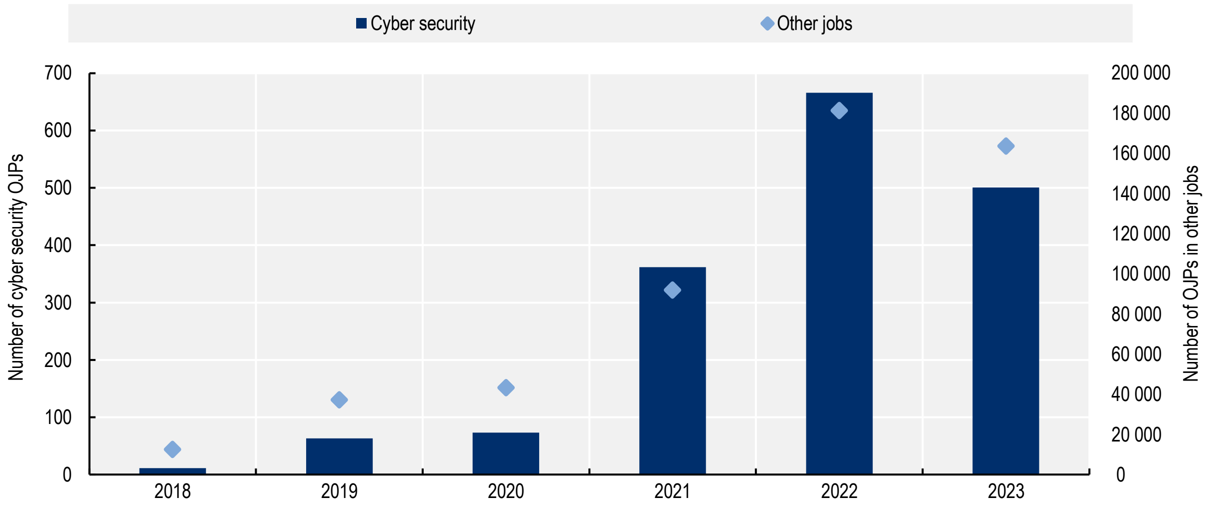


Source: OECD calculations based on Lightcast data.

More generally, just like France, Germany experienced a surge in the number of OJPs in both cyber security and non-cyber security jobs in 2020 during the height of the pandemic. However, unlike in France and Poland, the average number of monthly OJPs for both cyber and non-cyber positions decreased in 2021 (Figure 2.4) [7]. It is noteworthy, however, that the decrease in average monthly OJPs for cyber security roles in 2021 was lower than that for non-cyber jobs (Table 2.1). Among some of the potential explanations for this result, the surge in teleworking and its accompanied cyber risk led to higher demand for cyber security professions than for other professions as the "SARS-CoV-2 Occupational Safety and Health Ordinance" instituted in January of 2021 obligated employers to offer teleworking opportunities "in the case of office work or comparable activities, unless there were compelling operational reasons to the contrary." (Bundesministerium für Arbeit und Soziales, 2021[27])). This obligation was removed from the ordinance in March of 2022, but the share of employees that continued to work from home continued to be around 25% (IFO, 2022[28]).

The job market for cyber security roles, compared to non-cyber positions, has experienced the most substantial growth in Poland, as evident in Figure 2.3 and Table 2.1.[8] Differences in the starting size of the cyber security market in Poland, France, and Germany are likely reasons for variations in recent growth rates, as shown in Figure 1.2. The German market is more mature, with a larger share and a lower growth rate, while the Polish cyber security market is more up-and-coming. The demand for cyber security specialists in Poland initially trailed behind as evidenced by the low share of cyber security vacancies, the share increased significantly in the last five years, raising to levels that are now higher than in France by 2023.

Figure 2.5. Average monthly (cyber security) job postings in Poland



Source: OECD calculations based on Lightcast data.

Moreover, the Polish Government has actively implemented a cyber security policy in 2017, while 2018 marked the year of the adoption of the "Act on the national cyber security system", which created the legal and organisational basis for building a comprehensive cyber security system in Poland (Ministry of Digital Affairs, 2019[29]). The government developed a further national cyber security strategy in 2019 and made cyber security part of an integrated national security strategy which covered multiple domains (for more information see Box 2.4).

Additionally, Poland's cyber infrastructure is increasingly targeted by cyber-attacks, especially following the 2022 Russian invasion of Ukraine (ITA, 2023[30]). This has heightened the nation's risk awareness and likely driven an increased demand for cyber security experts. In 2022, Poland ranked 6th in Europe in terms of cyber threats, experiencing an average of 2 316 attacks per week on public institutions (ITA, 2023[30]).

Box 2.4. Poland's national cyber security strategy and policy

The primary goal of Poland's national security strategy (Ministry of Digital Affairs, 2019[29]) is to enhance resilience against cyber threats and protect information in public, military, and private sectors. The intention is also to promote knowledge and best practices for citizens in order to safeguard their information. More specifically, the government intends to develop their national cyber security scheme, including an evaluation of the National Cyber Security System Act. Additionally, it wants to increase the robustness of information systems in the public sector and within companies and achieve the capacity to prevent and respond to incidents effectively. The way of achieving this is for instance by implementing new cyber security standards for applications, mobile devices, servers and networks; establishing a national cyber security certification authority and increasing national capacity for research and development of state-of-the-art technologies and solutions in cyber security. The government also aims raise public awareness and competencies in cyber security and establish a strong international position in this field. This strategy elaborates on the national cyber security policy from 2017, which shared many of the same goals (Ministry of Digital Affairs, 2017[31]).

In May 2020, Poland integrated its cyber security objectives with the broader national security strategy, much like Germany did in 2023 (Government of Poland, 2020[32]). This document reiterates the government's goals to enhance resilience against cyber threats and information protection in public, military, and private sectors. However, it also mentions strengthening defensive capabilities, building capabilities for military operations in cyberspace, and developing testing and research capabilities for cyber security solutions. Furthermore, it mentions raising awareness of threats and challenges in cyber security and raising people's competences and knowledge to handle these situations. It also aims to develop Poland's national potential by coming up with domestic solutions through research and development in modern technologies.

Zoom in: What are the job roles in high demand within the cyber security landscape?

OJPs can provide a detailed overview of the demand for specific cyber security professionals/roles within the cyber security landscape. This section leverages text mining techniques applied to the job titles used by employers in job postings with the aim to categorise them into different roles, following the approach applied in recent OECD work (OECD, 2023[6]; OECD, 2023[7])[9]. The analysis focuses on four major roles: cyber security analysts, architects and engineers, auditors and advisors, and managers.

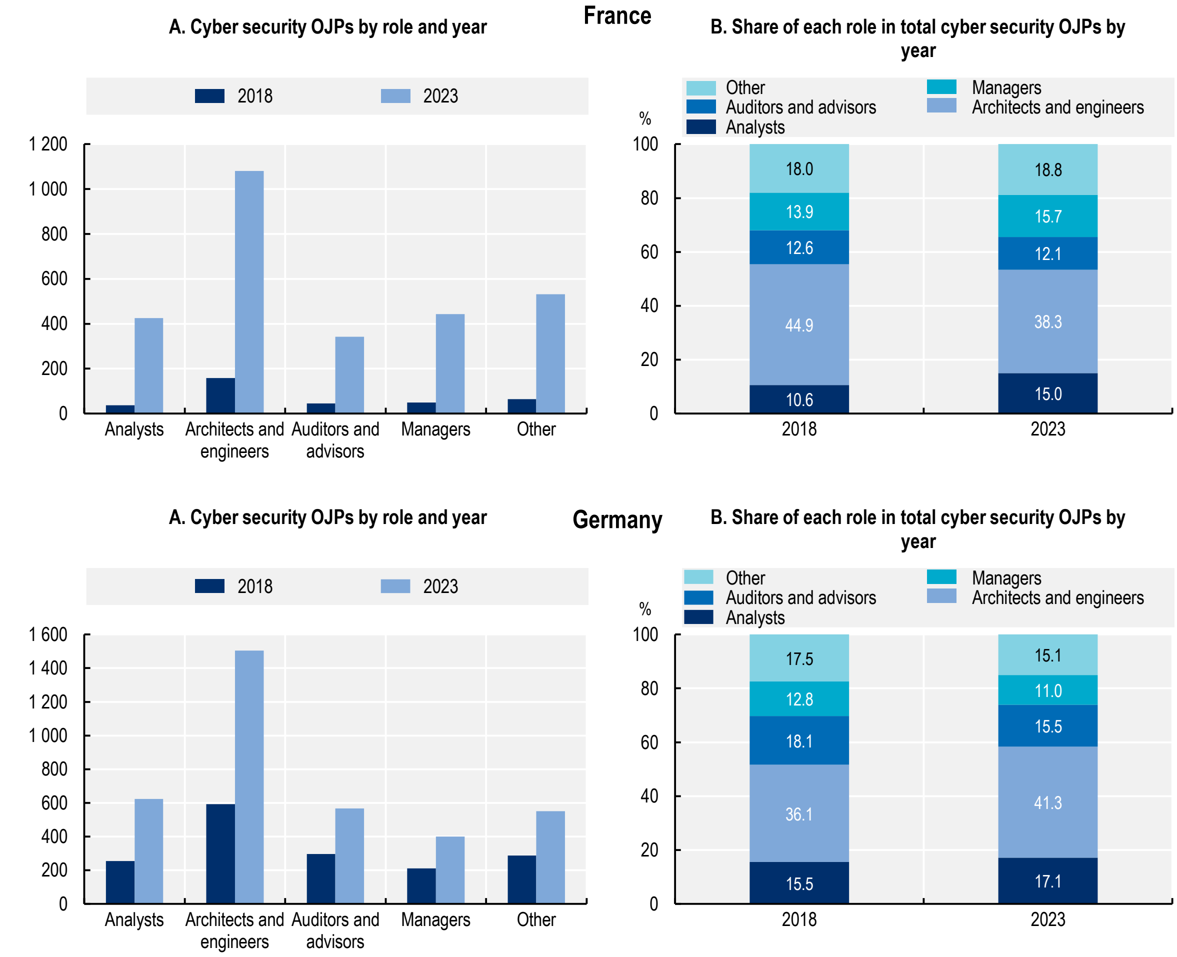
Results in Figure 2.6 and Figure 2.7 show that the distribution of the demand across different cyber security roles in France, Germany and Poland follows a pattern similar to the one observed in the Anglophone countries analysed in OECD (OECD, 2023[6]) and to the one observed in Latin America (OECD, 2023[10]). In both of those cases analysts and architects/engineers represented the majority of the total OJPs for cyber security professionals as well.

Cyber security architects are primarily responsible for designing security solutions that address business needs. According to the NICE Cyber Security Framework by NIST, architects securely provision IT systems, emphasising the design and modelling of security solutions (NICCS, 2023[33]). Engineers, on the other hand, closely collaborate with architects and focus on the processes required for implementing security solutions and integrating them with other IT products, as outlined by the Joint Task Force Transformation Initiative (2018[34]). Both architects and engineers play essential roles in developing comprehensive security solutions, configuring infrastructure, and integrating security technologies, ensuring digital infrastructure resilience against cyberattacks, and incorporating security measures into system and application design.

Across all three countries, job postings for architects and engineers consistently represented the largest share from 2018 to 2023. However, data show that there have been notable changes in the composition of the cyber security demand within countries and over time. In France, for instance, the share of OJPs seeking architects and engineers decreased from 44.9% in 2018 to 38.3% in 2023, while in Germany this increased by approximately 5 percentage points over the same period (Figure 2.6). France instead experienced a substantial surge in demand for cyber security analysts over the same years. Germany also experienced an increase in demand for analysts but, concurrently, there was a significant decline in the proportion of OJPs for auditors, going from 18.1% to 15.5%. Shifts in the demand within the groups of cyber security professionals underscore the evolving dynamics of the cyber security job market which is likely to reflect the adoption of new technologies, processes and priorities of firms.

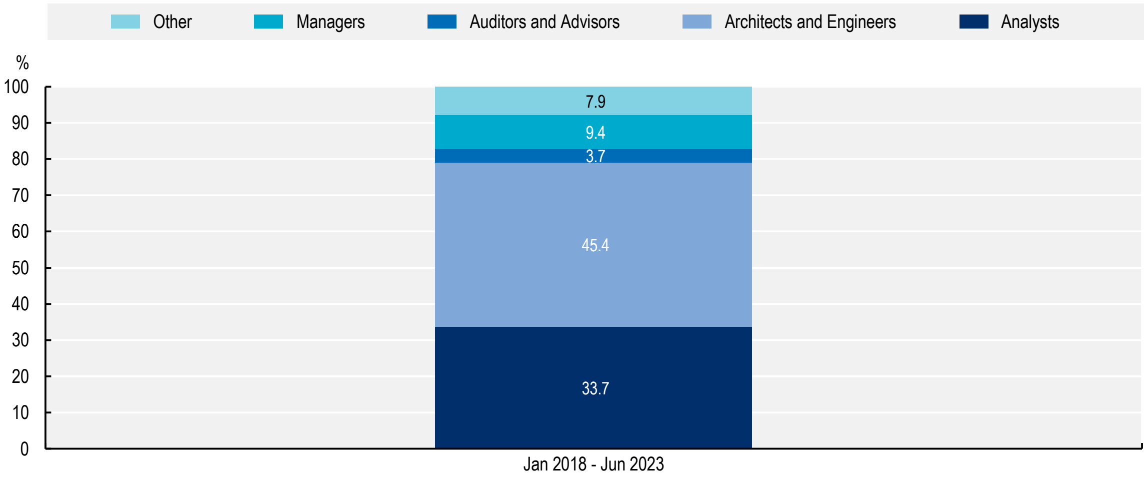
Similarly to results in (OECD, 2023[6]) and (OECD, 2023[10]) for most of the Anglophone and Latin American countries, cyber security analysts are the second most in-demand cyber security role in both Germany and Poland as well, with a large share of cyber OJPs seeking professionals in this role (Figure 2.6, Figure 2.7). Cyber security analysts play a pivotal role in the protection of digital assets and sensitive information. Their responsibilities involve extracting insights from diverse data sources to support the planning, operations, and maintenance of IT systems security (NICCS, 2022[35]). These professionals analyse and interpret security data, identify vulnerabilities, and implement measures to mitigate digital security risks. The NICE Cyber security Framework recognises their significance with a dedicated category, encompassing specialty areas like exploitation/vulnerability, language, and threat analysis (NICCS, 2023[36]).

Figure 2.6 Cyber security roles: Recent evolution and shares in France and Germany



Source: OECD calculations based on Lightcast data.

Figure 2.7. Cyber security roles: Average shares in Poland



Note: due to a limited number of online job postings per role in Poland per year, only the average composition across January 2018 and June 2023 is represented.
Source: OECD calculations based on Lightcast data.

In France, cyber security managers, which is the only managerial cyber role, instead is the second most highly sought after role within the cyber security labour market, with 15.7% of the total job postings in 2023 (Figure 2.6). According to the NICE Cyber security Framework, managers fall into the category of "oversee and govern," which includes all positions in charge of providing leadership, management, and direction to cyber security teams in an organisation. Specifically, this classification defines cyber security managers as professionals overseeing the cyber security programme of an information system or network and managing information security implications within different areas of responsibility (NICCS, 2023[36]). The relatively high demand for cyber security managers suggests a shifting landscape in the French cyber security labour market, indicating a growing emphasis on leadership and governance to effectively address cyber risk, complementing the technical expertise offered by cyber security analysts and engineers.

It is worth noticing that, in addition to the methodology in the two earlier reports in this series, (OECD, 2023[6]) (OECD, 2023[10]), this report also uses keywords related to the general data protection regulation (GDPR) into the strategy to classify cyber security job postings (see Annex 2.A). Given the geographical scope of the analysis, the European Union's (EU) General Data Protection Regulation (GDPR), for which compliance is obligatory for companies selling products/services in the European Union, becomes highly relevant. The GDPR sets forth guidelines for collecting, processing, and storing personal data for EU citizens (GDPR EU, 2022[37]). The EU's GDPR and other data privacy regulations place stringent requirements on organisations regarding the protection of personal data (GDPR EU, 2022[37]). Failure to comply can result in substantial fines, making data protection a critical aspect of cyber security.

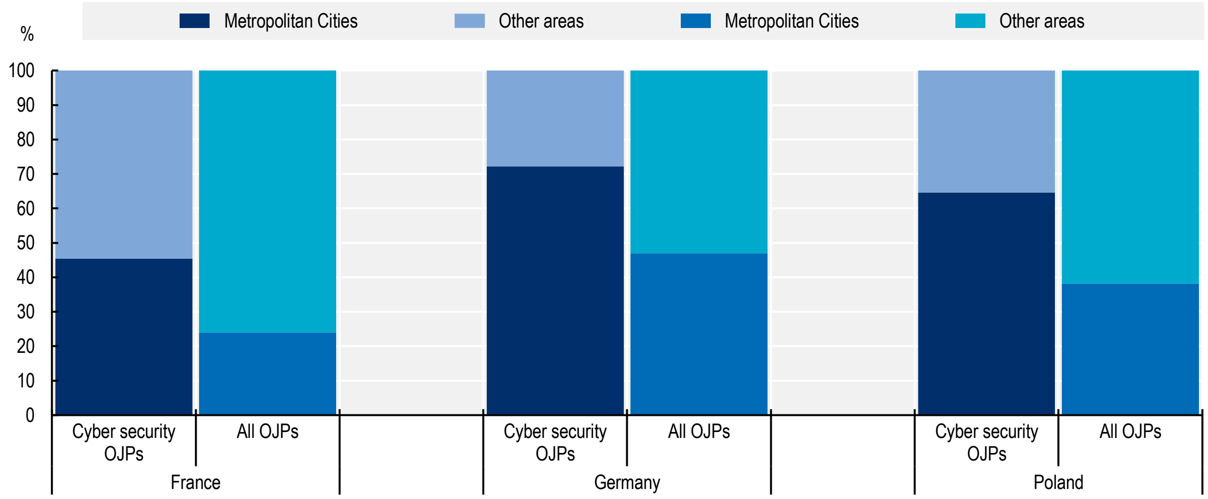
The inclusion of keywords that are associated with the GDPR into the classification, broadens the scope of cyber security roles to encompass positions like legal experts in GDPR compliance, experts in private data or data protection, and data protection consultants.[10] Notably, the inclusion of this relevant aspect of cyber security in the EU has contributed to a large share of demand for auditors and advisors in Germany between January 2018 and June 2023. This group accounted for an average of 17.4% of the total demand for cyber security professionals, a share which is nearly five times larger than in Poland and 5.7 percentage points larger than in France. Cyber security auditors and advisors encompass professionals dedicated to providing both internal and external guidance on the efficiency and compliance of security solutions. A high demand for auditors and advisors means that organisations acknowledge that cyber security encompasses not only the implementation of preventive measures but also the regular evaluation and verification of their effectiveness, as well as effectively incorporating legal frameworks.

Where is the demand for cyber security professionals located?

Job opportunities in the cyber sector are often geographically concentrated and it is worth examining the distribution of job opportunities for cyber security professionals by comparing the share of cyber security job postings in metropolitan cities to those in other regions. Previous research also indicates that job opportunities for cyber professionals are predominantly concentrated in larger cities (OECD, 2023[6]) (OECD, 2023[10]). In this analysis, metropolitan cities are defined as cities with a population of 250 000 inhabitants or more. According to the latest census data, there are 139 metropolitan cities in France[11], 63 in Germany, and 11 in Poland, constituting 15%, 22%, and 17.6% of the population, respectively (INSEE, 2023[38]; Statistics Poland, 2023[39]; Statistische Ämter des Bundes und der Länder, 2023[40]).[12]

In all three countries, the proportion of cyber security OJPs in metropolitan cities significantly exceeds that of non-cyber OJPs, as illustrated in *(*Figure 2.8*).*[13] This outcome aligns with expectations, as previous reports also found that cyber security is typically in high demand within major urban areas, where prominent enterprises and government agencies often have their headquarters (OECD, 2023[6]; OECD, 2023[7]). Within larger cities, financial, technological, industrial, governmental, and other sectors often have a large presence. These sectors necessitate secure IT services and infrastructure, along with a skilled workforce capable of safeguarding their operations. The disparity between cyber and non-cyber occupations is most pronounced in France, where the share of cyber security OJPs in metropolitan cities is 1.9 times larger than that of all OJPs. However, in Poland and Germany, the differences are similar, at 1.7 and 1.5 times, respectively. The French Government has recently invested greatly into cyber security in Paris specifically, by building a large cyber campus which opened in 2022 (see Box 2.5).

Figure 2.8. Share of online job postings (OJPs) in metropolitan cities versus in other areas



Note: Metropolitan cities are cities with 250 000 inhabitants or more. In the case of France, communes within the Greater Paris region are also counted as metropolitan cities. Online job postings (OJPs) for which the location was not reported are excluded from the analysis, 26%, 25.8% and 19.1% in France, Germany and Poland respectively.
Source: OECD calculations based on data from Lightcast.

Box 2.5. Enhancing cyber ecosystems in Paris and other regions in France: Campus Cyber

France’s economic landscape is heavily concentrated in Paris, as approximately 31% of the nation's GDP is generated within the Greater Paris region (L'institut Paris Region, 2023[41]). This concentration extends to the labour market for cyber security, with a notable 27.4% of all cyber security OJPs being situated in this region. Recent initiatives by the French Government, such as the proposal to establish a cyber campus in the financial district of La Défense may further centralise the labour market for cyber security professionals.

In 2021, the French Government announced “*Campus Cyber*” project, an initiative that aims to foster collaboration among companies, government departments, training organisations, and research institutes by locating them in the same facility (ANSSI, 2021[42]). It first opened its doors in 2022. The campus serves as part of the government’s broader cyber security plan, which involves substantial investments of approximately EUR 1 billion into the cyber security sector (Gouvernement de la France, 2021[43]). The Campus Cyber project is anticipated to bring together around 1 600 professionals (Demagny, 2022[44]), which, for context, accounts for approximately 5% of the total number of cyber security OJPs in 2022.

The Campus Cyber governance is the main driver to stimulate the expansion of Territorial Campuses within the French territory. Indeed, eleven of the French regions had already joined the National Campus Cyber governance. This is the first step, to create, at a national scale, an operational territory network where every region will be able to create their own Campus Cyber.

In fact, each territorial cyber security ecosystem possesses its own specialisations and sectors of excellence. The main goal is to create specialised working groups at a local level and then share the expertise between the national and all the regional campuses. This framework will allow the whole ecosystem to push forward strategic topics based on each region's strength, thus levelling on a national scale the level of innovation in cyber security.

Since 2022, the Hauts-de-France, Nouvelle-Aquitaine and Bretagne regional Campuses Cyber have been inaugurated as Territorial Campus Cyber. For now, five others are on a good track to open their doors in the coming year and be labelled.

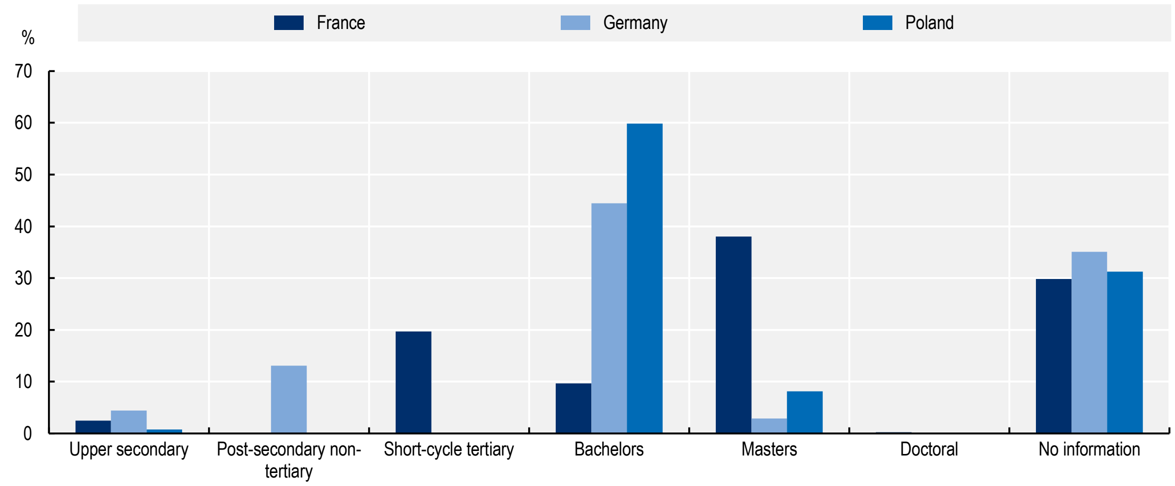
The professional profile required in cyber security online job postings

This section explores some of the characteristics that define the profile sought by enterprises in the cyber security labour market. Using a text mining approach, the analysis looks into the qualifications required by firms in different countries to fill cyber security positions. Additionally, utilising a machine learning approach, it identifies the essential professional and technical skills relevant to the field, with a particular emphasis on the latest emerging technologies demanded by enterprises.

Qualification requirements in cyber security online job postings

Qualifications are among some of the key aspects that enterprises use to select qualified candidates in the cyber security job market. In order to analyse education requirements, this report employs text mining techniques applied to OJPs in the year 2022 (see Annex 2.C). It is worth noting that, while education requirements are not available for significant share of the OJPs considered in this report the available information is still of great help to characterise the cyber security workers' profile by retrieving the typical educational degrees demanded by firms across labour markets over thousands of different job postings. The shares of OJPs without explicit education requirements range between 30% and 35% (Figure 2.9). This is likely due in part to employers increasingly focusing on experience and on informal forms of education to signal cyber security skills instead of requiring formal degrees.

Figure 2.9. Education requirements in terms of ISCED in OJPs



Note: The International Standard Classification of Education (ISCED) provides a classification of education requirements that is comparable across the world (see Box 2.6).
Source: OECD calculations based on Lightcast data.

Results indicate that across all three countries analysed in this study, enterprises typically look for cyber security workers with tertiary education (ranging between 73% and 99% of the job postings for which education requirements are published).

Figure 2.9 shows that bachelor's degree is the most prevalent education requirement in both Germany and Poland. The different education levels in Figure 2.9 described in more detail in Box 2.6. In Poland, 87.1% of job postings specifying education requirements request a bachelor's degree, with 11.8% requesting a master's degree. In Germany, 68.4% of job postings require a bachelor's degree, with an additional 4.4% seeking candidates with a master's degree. This emphasis on bachelor's degrees is a prevailing trend in these highly technical professions. A similar pattern was observed in English-speaking countries, with 83% of the job postings reflecting this trend (OECD, 2023[6]). Notably, (ISC)² characterises a cyber security professional as an individual with a strong educational background, with 86% of respondents holding at least a bachelor's degree or higher ((ISC)2, 2021[45]).

By contrast, the majority (54.2%) of French employers that explicitly mention an educational requirement in their vacancies for cyber security professionals, request a master's degree. Interestingly, the demand for master's degrees in France is about 12 times larger than in Germany and 4.6 times larger than in Poland. At the same time, the share of job postings that seeks candidates with a bachelor's degree is much lower in France than in Germany and Poland, accounting for just 13.8% of those with explicit requirements. As is shown in Chapter 3, enrolment in cyber security education is highly focused in higher education programmes including bachelor's and master's degrees. Most of the positions open to candidates with ISCED level 7 education advertise that candidates need to have "bac + 5" or have obtained a diploma from an engineering school (*l'école d'ingénieurs*). "Bac + 5" signifies five years of education following the acquisition of a high school diploma, which is equivalent to obtaining a master's degree. Engineering schools in France provide education in technical subjects, like informatics and cyber security, at a master's level and produce approximately 35 000 graduates every year (Government of France, 2018[46]).

Additionally, a significant share of job postings in France requests short-cycle tertiary education (28.1% of OJPs with explicit education requirements). In France, this type of education is more prevalent than in other countries, with 12% of individuals having obtained it (OECD, 2023[7]). In some countries, such as Poland programmes at the ISCED 4 and 5 levels do not exist. These educational paths lead to degrees known as "*brevet de technicien supérieur"* (BTS) or "*Diplôme universitaire de technologie"* (DUT) (Box 2.6). These types of qualifications are often offered at "university institutes of technology". Most cyber security positions that specify this type of education are related to system administrator and technician positions. Short-cycle tertiary education is, instead, rare in Germany and Poland and only 0.4% and 0.1% of the German and Polish population respectively hold such degrees (OECD, 2023[7]).

Figure 2.9 shows that in contrast to France and Poland, a significant share of OJPs in Germany (20.2% of those with explicit education requirements) seek candidates with post-secondary non-tertiary education. Data for Germany show, for instance, that employers look for candidates who have completed an "*Ausbildung,"*, a vocational training programme, typically at a vocational school. This form of education is often pursued alongside employment with a company, resulting in both a diploma and valuable work experience. Cyber security OJPs requesting ISCED level 4 qualifications in Germany also commonly emphasise the importance of practical experience and sometimes even offer support in obtaining further qualifications.

Box 2.6. Different levels of education

The education requirements in the OJPs can be translated into levels that are in accordance with the International Standard Classification of Education (ISCED) (see Annex 2.C). ISCED provides a classification that is comparable between all countries of the world (UNESCO, 2018[47]). ISCED comprise nine different levels, but levels 0-2 are never demanded in the cyber security OJPs. The other levels are as follows (UNESCO, 2018[47]):

- **ISCED 3: Upper secondary education.** Programmes in the ISCED level 3 are typically designed to complete secondary education in preparation for tertiary education or to provide skills relevant to employment, or both.
- **ISCED 4: Post-secondary non-tertiary education.** This level provides learning experiences building on secondary education, and usually facilitates direct labour market entry. Post-secondary non-tertiary education programmes aim at the acquisition of knowledge, skills and competencies lower than the level of complexity characteristic of tertiary education. In France, education at this level is almost non-existent (European Commission, 2022[48]), while in Germany for instance one-year courses at *Fachoberschulen* and the two-year courses at *Berufsoberschulen/Technischen Oberschulen/Berufsfachschulen* count as ISCED level 4 (European Commission, 2023[49]). In Poland schools at this level are often called *szkoła policealna* (European Commission, 2023[50]).
- **ISCED 5: Short-cycle tertiary education.** Programmes categorised in ISCED level 5 are often designed to provide participants with professional knowledge, skills and competencies. Typically, they are practically based, occupation-specific and prepare students to enter the labour market. Academic tertiary education programmes below the level of a bachelor's programme or equivalent are also classified as ISCED level 5. In France, this level includes the *Diplôme universitaire de technologie* (DUT), a two-year degree at a technical institute that was available between 1966 and 2021. The DUT has been replaced by the *Bachelor universitaire de technologie* in 2022, which instead is considered ISCED level 6 (European Commission, 2022[48]).In the OJPs for France in 2022, however, DUT is still present among the education requirements.
- **ISCED 6: Bachelor's or equivalent level.** Programmes at ISCED level 6 aim to provide participants with intermediate academic and/or professional knowledge, skills and competencies. They are traditionally offered by universities and equivalent tertiary educational institutions.
- **ISCED 7: Master's or equivalent level.** Programmes at ISCED level 7 provide participants with advanced academic and/or professional knowledge, skills and competencies. Programmes at this level may have a substantial research component but do not yet lead to a doctoral qualification.
- **ISCED 8: Doctoral or equivalent level.** Programmes at ISCED level 8 are designed primarily to lead to an advanced research qualification.

The skills bundle of cyber security professionals

The extensive adoption of digital technologies, along with the emergence of new cyber threats is reshaping the skill requirements for cyber security professionals. This dynamic and highly technical landscape presents challenges for both the demand and supply sides of the labour market, creating a shortage of skilled and qualified individuals in the job market who can effectively fulfil roles in cyber security and adequately address a variety of cyber threats. While shortages in the field have been well-documented over the years, they continue to have a significant impact on countries throughout Europe and worldwide (ENISA, 2021[3]). Within individual countries and specific sectors, these challenges can be even more pronounced due to intense competition for a limited number of security professionals. This often results in certain sectors, such as governments and central banks, struggling to attract highly skilled security professionals compared to other sectors, like the finance industry, which can offer more financially rewarding employment opportunities (ENISA, 2021[3]).

To formulate policies that effectively bridge the cyber security skills gap, there is a need for comprehensive data that accurately characterises the demand and supply of skills in this sector. Traditional labour market data, while valuable, often lack the granularity and timeliness needed to provide a nuanced understanding of this dynamic landscape. The analysis of online job postings can help foster such an understanding, equipping policy makers with insights into the precise skills that are in demand within the cyber security field. This, in turn, enables policy makers to tailor their capacity-building efforts, respond to evolving labour market needs, and foster a skilled workforce that can thrive in the dynamic cyber security landscape.

This section examines the specific skill requirements mentioned by employers in cyber security online job postings. In particular, the analysis presented in Figure 2.10 employs Natural Language Processing (NLP) techniques (see Box 2.7) to identify the most relevant technical and professional skills required by employers seeking cyber security professionals in each country analysed. Technical skills refer to specialised knowledge or expertise required to perform specific tasks within the profession, while professional/transversal skills encompass broader skills not limited to a particular job or discipline but applicable in various situations or work environments.[14]

Box 2.7. Using machine learning to assess the relevance of skills in cyber security occupations

Recent advances in machine learning techniques led to the development of language models which have the objective of understanding the complex relationships between words (their semantics) by deriving and interpreting the context those words appear in. Language models (in particular Natural Language Processing, NLP, models) interpret text information by feeding it to machine learning algorithms that derive the logical rules to interpret the semantic context in which words appear.

NLP models are therefore better suited for the analysis of text information. As such, they are used for the analysis of OJPs in this section of this report. These algorithms allow the calculation of semantic similarity measures between skills and occupations. Skills that are more semantically similar to a certain occupation are interpreted as being more ‘relevant’ to the occupation (see Annex 2.A for methodological details).

Results in Figure 2.10 indicate that transversal skills are typically much less relevant than technical skills in cyber security job postings in Germany and Poland, while in France both types of skills often hold near equal significance. Professional skills have reportedly gained importance in the cyber security sector, for instance, a report on the state of the cyber security profession indicates that 54% of the surveyed managers report deficiencies in ‘soft’ skills among cyber professionals (ISACA, 2022[51]). This underscores the importance for cyber security professionals to possess both technical and professional skills in order to meet the requirements set up by employers.

This report has expanded which roles are classified as cyber security jobs, by including highly relevant keywords on data protection and GDPR. This has resulted in the emergence of a wider range within the important skills as depicted in Figure 2.10 than in (OECD, 2023[6]) (OECD, 2023[10]). For instance, the skills “managing IT security compliances” in France is highly relevant. In line with the notable presence of auditors and advisors in Germany, knowledge of ICT security legislation and standards, along with information security strategy skills, are even the three most relevant skills found in the OJPS for German cyber security professionals. These skills go beyond programming abilities or familiarity with certain software or tools, but instead encompass legal and regulatory aspects.

Programming and familiarity with software and digital tools is paramount in the three countries analysed. In Germany for instance, cloud technologies such as Microsoft Azure show high relevance for cyber security personnel in the demands of employers. In France and Poland, instead familiarity with the technology “Cisco” is often asked from cyber security professionals. In Poland, OJPs for cyber security personnel frequently use the keywords “cloud technologies” (without specifying a particular technology). This is in line with analyses by the (ISC)^2 that emphasise cloud computing security among the most relevant skills for cyber security professionals ((ISC)2, 2021[45]).

Zooming in on France, cyber security personnel are often asked for knowledge on “applying operations in an ITIL based environment”. The Information Technology Infrastructure Library (ITIL) is a widely adopted framework for IT service management (Axelos, 2023[52]), which has five so-called service operations processes. Although ITIL does not have an emphasis on cyber security, it provides guidance for organisations in managing their IT services. By incorporating ITIL into their cyber security practices, organisations can establish robust incident/event management processes, ensure proper access management and align IT security management efforts with overall IT service management objectives (Coursera, 2023[53]).

In Poland, the most sought-after skills revolve around areas like ICT networking hardware, virtual private network implementation, and web programming. This aligns with the predominant demand for architects and engineers in the field, which accounted for an average of 45% of cyber-related OJPs between January 2018 and June 2023. This trend also likely reflects Poland’s focus on technical proficiency and infrastructure management in the realm of cyber security.

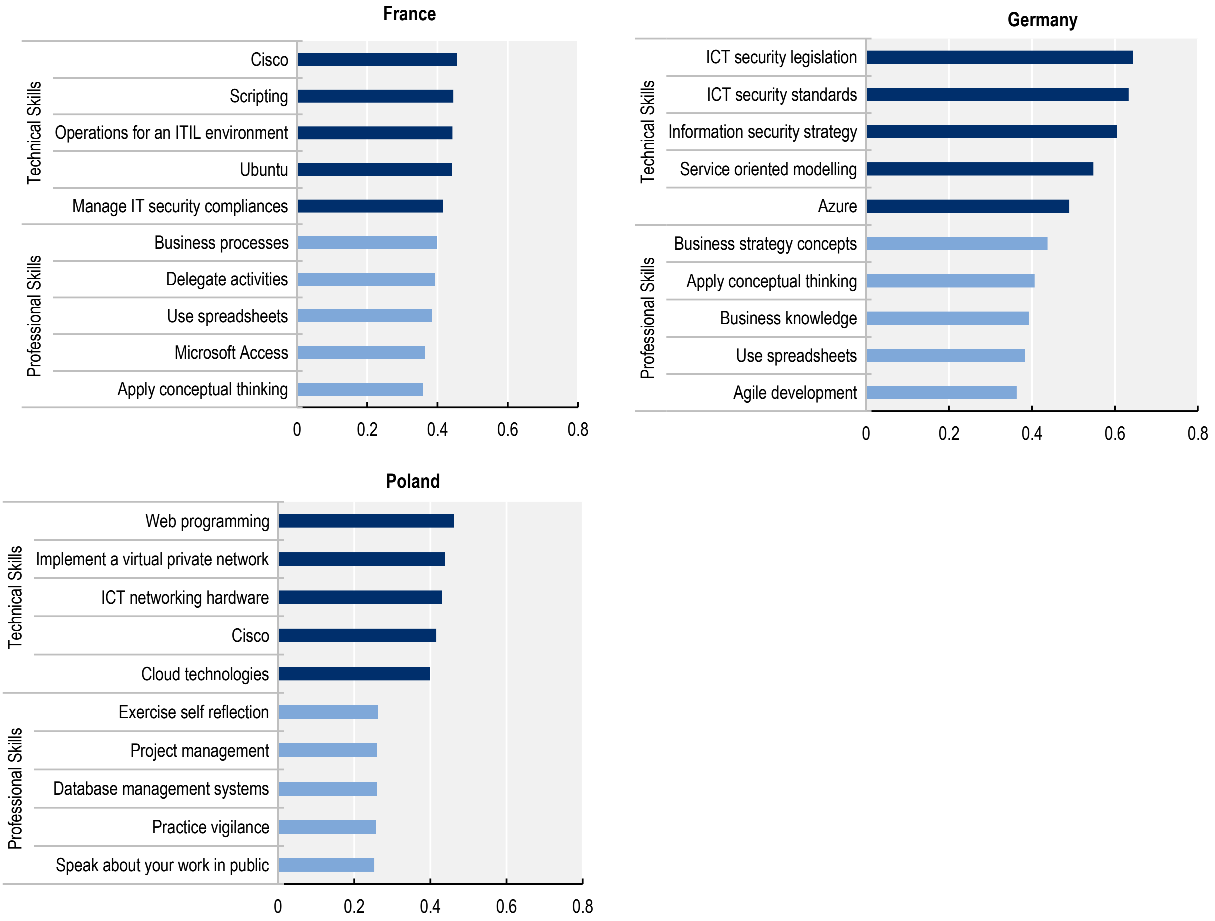
Overall, according to (ISC)^2, professionals within the cyber security market are expected to combine technical expertise (such as proficiency in programming, cloud computing, and IT infrastructures) with security strategy skills (including governance, risk assessment and compliance or threat intelligence) ((ISC)2, 2021[45]). This allows them to develop security systems that not only shield businesses from cyber threats but also ensure compliance with internal and external regulations. This multifaceted mix of skills can be found in cyber OJPs in France, Germany, and Poland as well.

When focusing the analysis on the demand for professional skills, instead of technical skills, OJPs in France and Germany primarily ask for conceptual thinking, proficiency in spreadsheets, and an understanding of business processes (Figure 2.10). Given the ever-evolving nature of cyber threats, professionals in this field need to continually adapt and evolve their techniques and approaches to tackle emerging challenges. Conceptual thinking forms a cornerstone for implementing technical solutions against cyber threats. Interestingly, in Poland, there is instead a more pronounced emphasis on self-reflection, vigilance, and public speaking.

In contrast to the findings presented in (OECD, 2023[10]), explicit demand for English language skills is not among the skills with the highest relevance in the European cyber OJPs, even though English is not the native language in any of the three countries. These European countries have generally achieved a good proficiency in English, with for instance Germany and Poland ranking among countries with very high proficiency, and France as moderate proficiency (EF, 2022[54]). That being said, despite being an implicit requirement in cyber security jobs in Europe, it is important to notice that proficiency in English language ensures that potential barriers to skill development are minimal, given that the majority of relevant training materials, industry standards, and certifications are predominantly available in this language.

Figure 2.10. Skill bundle demands in the cyber security profession

Skills with the highest relevance for the cyber security profession in 2022 (closer to 1 = more relevant)



Note: The relevance scores are derived from the semantic analysis of online job postings for each country in 2022. The closer the score to 1, the more relevant the skill for the cyber security occupation in the country at hand. For more details on the methodology see Annex 2.D.
Source: OECD calculations based on Lightcast data.

Are cyber security skills demands becoming more specialised?

Labour markets evolve rapidly, and the intensity of skill demands can change over time. While some skills may become more mainstream and demanded in a wider range of occupations, other skill demands may remain niche and concentrated in a specific set of occupations for a long time. Most cyber security-related skills are highly technical and it is interesting to see whether the demand for these is diffusing across the labour market more generally or whether the demand remains concentrated in more technical and cyber-related occupations.

The analysis in this section uses machine learning indicators (see Box 2.8, Annex 2.A and Annex 2.D) to evaluate the information contained in OJPs in between 2019 and 2022. This is done in order to assess whether the demand for different types of cyber security skills has been diffusing across an increasing number of non-technical/non-cyber occupations or whether, instead, these demands have become more concentrated in a narrower set of cyber and technical occupations.

Box 2.8. Assessing the connectedness of cyber security skill demands using machine learning

The information contained in online vacancies is textual in nature. Natural Language Processing algorithms (NLP) can be used to make sense of it by transforming the semantic information into mathematical vectors that can be understood and analysed by a machine (see Annex 2.A). Those mathematical vectors (which are meant to retain the meaning of the words they represent) occupy a specific place in a mathematical high-dimensional space, this latter commonly referred to as a 'graph'.

When keywords, in this case 'skills', are converted into vectors in a graph, it is possible to measure the degree by which they are connected with each other (when keywords co-occur in a specific job vacancy) or disconnected (when they never co-occur in the same vacancy). In graph theory, the "eigenvector centrality" is a measure that is commonly used to assess the influence of a node in a network or, in other words, to measure the degree and quality of connections of a keyword with the rest of words in the text under exam.

Originally, this measure was developed by researchers in Google and used in the PageRank algorithm to quantify the importance of the connections among web pages based on the textual/semantic information contained in it (Brin and Page, 2012[55]). The same measure can, however, be used to capture the number of connections that a skill keyword has with other skills across the 'corpus' of OJPs. This study uses eigenvector centrality (Annex 2.D) to measure how well-connected (i.e. pervasive) each skill is in the labour market in a specific point in time. This, in turn, allows to calculate whether a certain skill has become more or less connected (i.e. less or more concentrated) during the period under examination. This is done by calculating the change in the eigenvector centrality scores in two periods of time and benchmarking this change by the average change in eigenvector centrality in the same period.

Source: OECD (2022[9]), *Skills for the Digital Transition. Assessing Recent Trends Using Big Data*, https://doi.org/10.1787/38c36777-en.

Whether the demand for a certain skill becomes more mainstream (i.e. "more diffused across occupations") or, instead, more specialised (i.e. "with fewer connections with other skill demands") is likely to be determined by the complexity of the skill under consideration. For instance, while the demand for basic digital skills is likely to be spreading to a wider range of occupations at a fast pace (including non-technical occupations), other- more sophisticated - digital skills (such as the cyber security-related ones) may remain the domain of very technical occupations.

Table 2.2 highlights an interesting trend: data for both France and Germany show that the demand for cyber security skills[15] has become increasingly more concentrated and specialised. In other words, the number of 'connections' (see Box 2.8) between cyber security skills and other skills across the whole database of OJPs has become smaller, signalling that keywords connected to cyber security skills are prevalently found in a narrow set of work contexts and occupations. This result holds also when comparing these connections with the average skill in the database, meaning that the majority of the cyber security skills have become more specialised and at a faster pace than the average skills in the examined economies.

While caveats apply to this analysis as time series used in this report are not very long, results show that the pace of change is most rapid in France, indicating that cyber security skills are becoming more concentrated at a significantly higher rate when compared to the average skill in the labour market. Furthermore, the data show that the skill "cyber security" is significantly less well-connected than the average skill in both 2019 and 2022, reinforcing the notion that it is only required within a limited and specific subset of jobs. In Germany, results also indicate that the demand for cyber security skills is increasingly becoming more targeted to a narrow set of OJPs, though to a lesser extent than in France.

Results for Poland show, instead, a different trend. The analysis shows that the skill keyword "cyber security" has become more connected over time, being used in a wider range of OJPs in different occupations and mentioned with a wider set of other skill keywords. This result is likely related to the fast expanding cyber-security sector in Poland which started very small (and very concentrated) at the beginning of the period and grew significantly in recent years to encompass a larger set of roles.

Table 2.2. Skills that are explicitly cyber security related

France	Skills demand specialisation index	Germany	Skills demand specialisation index	Poland	Skills demand specialisation index
Cyber security	1.410	Cyber security	0.852	Cyber security	-0.039
ICT security standards	1.173	ICT security standards	0.628		
Manage IT security compliances	1.022	Manage system security	1.949		
Web application security threats	1.081	Web application security threats	1.650		
		ICT security legislation	0.672		
		Information security strategy	0.655		

Note: The skills demand specialisation index measures the extent by which a skill is increasing (respectively decreasing) its connectedness with other skills analyse across the whole database of online job postings. This is calculated as the change in the eigenvector centrality scores in two periods of time. This value is benchmarked to the average change in eigenvector centrality in the same period (see Box 2.8). Positive (respectively negative) values indicates that the demand for the skill under consideration has become more (respectively less) concentrated in a specific set of occupations. Values above 1 indicate that the skill is becoming more specialised at a rate that is faster than that of the average skill in the analysed economy.
Source: OECD calculations based on Lightcast data.

References

(ISC)2 (2023), *2023 Cybersecurity Workforce Study*, https://www.isc2.org/Research (accessed on 15 January 2024). [1]

(ISC)2 (2021), *Cybersecurity Workforce Study 2021. A Resilient Cybersecurity Profession Charts the Path Forward*, https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx. [45]

Adăscăliței, D. and T. Weber (2021), *The pandemic aggravated labour shortages in some sectors; the problem is now emerging in others*, http://eurofound.link/ef21082 (accessed on 18 September 2023). [66]

ANSSI (2021), *Un Campus Dédie À La Cybersecurité*, https://www.ssi.gouv.fr/agence/cybersecurite/un-campus-dedie-a-la-cybersecurite/ (accessed on 4 September 2023). [42]

ANSSI (2011), *Information systems defence and security - France's strategy*, https://www.ssi.gouv.fr/presse/communiques-de-presse/ (accessed on 3 November 2023). [19]

Axelos (2023), *ITIL® 4: the framework for the management of IT-enabled services*, https://www.axelos.com/certifications/itil-service-management/ (accessed on 1 June 2023). [52]

Brin, S. and L. Page (2012), “Reprint of: The anatomy of a large-scale hypertextual web search engine”, *Computer Networks*, Vol. 56/18, pp. 3825-3833, https://doi.org/10.1016/j.comnet.2012.10.007. [55]

Bundesministerium für Arbeit und Soziales (2021), *ARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV)*, https://www.bundesanzeiger.de/pub/publication/5QH1uegEXs2GTWXKeln/content/5QH1uegEXs2GTWXKeln/BAnz%20AT%2022.01.2021%20V1.pdf?inline (accessed on 4 September 2023). [27]

Cammeraat, E. and M. Squicciarini (2021), “Burning Glass Technologies’ data use in policy-relevant analysis: An occupation-level assessment”*, OECD Science, Technology and Industry Working Papers*, No. 2021/05, OECD Publishing, Paris, https://doi.org/10.1787/cd75c3e7-en. [5]

CBI (2022), *The European market potential for software development services*, https://www.cbi.eu/market-information/outsourcing-itobpo/software-development-services/market-potential (accessed on 4 October 2023). [14]

CCDCOE (2020), *National Cybersecurity Organisation: Germany*, https://ccdcoe.org/uploads/2020/12/Country_Report_DEU.pdf (accessed on 28 September 2023). [23]

CNIL (2022), *L’espace numérique de santé (ENS ou Mon espace santé) et le dossier médical partagé (DMP) : questions-réponses*, https://www.cnil.fr/fr/lespace-numerique-de-sante-ens-ou-mon-espace-sante-et-le-dossier-medical-partage-dmp-questions (accessed on 17 October 2023). [11]

Coursera (2023), *What Is ITIL? A Beginner’s Guide to the ITIL Process*, https://www.coursera.org/articles/what-is-itil (accessed on 5 May 2023). [53]

Dares (2022), *Télétravail durant la crise sanitaire - Quelles pratiques en janvier 2021? Quels impacts sur le travail et la santé?*, https://dares.travail-emploi.gouv.fr/sites/default/files/5171e9d0f2d214774c44afc82353563a/Dares-Analyses_Teletravail-durant-crise-sanitaire-Partiques-Impacts.pdf (accessed on 4 September 2023). [17]

Demagny, X. (2022), *Qu’est-ce que le campus cyber, inauguré ce mardi à la Défense ?*, https://www.radiofrance.fr/franceinter/qu-est-ce-que-le-campus-cyber-inaugure-ce-mardi-a-la-defense-8773053 (accessed on 19 September 2023). [44]

EF (2022), *EF English Proficiency Index - 2022 Edition*, https://www.ef.com/assetscdn/WIBIwq6RdJvcD9bc8RMd/cefcom-epi-site/reports/2022/ef-epi-2022-english.pdf (accessed on 17 October 2023). [54]

ENISA (2021), *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education/ (accessed on 4 September 2023). [3]

European Commission (2023), *Germany - Secondary and post-secondary non-tertiary education*, https://eurydice.eacea.ec.europa.eu/national-education-systems/germany/post-secondary-non-tertiary-education (accessed on 16 October 2023). [49]

European Commission (2023), *Poland - Upper secondary and post-secondary non-tertiary education*, https://eurydice.eacea.ec.europa.eu/national-education-systems/poland/upper-secondary-and-post-secondary-non-tertiary-education (accessed on 25 October 2023). [50]

European Commission (2022), *France - Secondary andn post-secondary non-tertiary education*, https://eurydice.eacea.ec.europa.eu/national-education-systems/france/secondary-and-post-secondary-non-tertiary-education (accessed on 16 October 2023). [48]

Fadic, M. et al. (2019), "Classifying small (TL3) regions based on metropolitan population, low density and remoteness"*, OECD Regional Development Working Papers*, No. 2019/06, OECD Publishing, Paris, https://doi.org/10.1787/b902cc00-en. [59]

Federal government of Germany (2023), *Robust. Resilient. Sustainable. Integrated Security for Germany - National Security Strategy*, https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf (accessed on 18 November 2023). [26]

Federal government of Germany (2021), *Cyber Security Strategy for Germany*, https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html (accessed on 6 November 2023). [25]

Federal Ministry of the Interior and Community (2021), *Cyber Security Strategy for Germany*, https://www.bmi.bund.de/EN/topics/it-internet-policy/cyber-security-strategy/cyber-security-strategy-node.html (accessed on 25 September 2023). [24]

French government (2023), *Communique de Presse - France 2030* | *Le Gouvernement lance une nouvelle vague de l'appel à projets pour*, https://www.economie.gouv.fr/files/files/2023/communique_AAP_cybersecurite.pdf (accessed on 6 November 2023). [22]

French government (2023), *Stratégie nationale « Cybersécurité » de France 2030 : deux nouveaux projets lancés dans le cadre du Programme de recherche (PEPR)*, https://www.gouvernement.fr/strategie-nationale-cybersecurite-de-france-2030-deux-nouveaux-projets-lances-dans-le-cadre-du (accessed on 16 November 2023). [21]

French government (2022), *Stratégie nationale d'accélération pour la cybersécurité : les premières réalisations*, https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite (accessed on 16 November 2023). [20]

GDPR EU (2022), *Does the GDPR apply to companies outside of the EU?*, https://gdpr.eu/companies-outside-of-europe/ (accessed on 15 May 2023). [37]

German Federal Foreign Office (2023), *Industrieland Deutschland – die wichtigsten Fakten*, https://www.deutschland.de/de/topic/wirtschaft/deutschlands-industrie-die-wichtigsten-zahlen-und-fakten (accessed on 30 October 2023). [12]

Gouvernement de la France (2021), *Un plan à 1 milliard d'euros pour renforcer la cybersécurité*, https://www.gouvernement.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite (accessed on 16 September 2023). [43]

Government of France (2018), *Les formations d'ingénieur*, https://www.enseignementsup-recherche.gouv.fr/fr/les-formations-d-ingenieur-46426 (accessed on 30 October 2023). [46]

Government of Poland (2020), *National Security Strategy of the Republic of Poland 2020*, https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf (accessed on 16 November 2023). [32]

IFO (2022), *In Germany, Number of People Working from Home Barely Lower despite End of Remote-Working Obligation*, https://www.ifo.de/en/press-release/2022-05-09/germany-number-people-working-home-barely-lower-despite-end-remote-working (accessed on 11 September 2023). [28]

INSEE (2023), *Employment, Unemployment, Earned income 2022 Edition*, https://www.insee.fr/en/statistiques/7455561?sommaire=7455576 (accessed on 16 October 2023). [63]

INSEE (2023), *Évolution et structure de la population en 2020 - Commune - France hors Mayotte*, https://www.insee.fr/fr/statistiques/7632446?sommaire=7632456#consulter (accessed on 4 September 2023). [38]

International Labour Organization (n.d.), *Updating the International Standard Classification of Occupations (ISCO) - Draft ISCO-08 Group Definitions: Occupations in ICT*, https://www.ilo.org/public/english/bureau/stat/isco/docs/d2434.pdf (accessed on 23 April 2023). [56]

ISACA (2022), *State of Cybersecurity 2022: Global Update on Workforce Efforts, Resources and Cyberoperations*, https://www.isaca.org/go/state-of-cybersecurity-2022. [51]

ITA (2023), *ICT Cyberattacks In Poland Take Place Every 9 Minutes*, https://www.trade.gov/market-intelligence/poland-ict-cyberattacks-poland-take-place-every-9-minutes#:~:text=According%20to%20Noventiq%20analysts%2C%20today,week%20to%202316%20per%20week. (accessed on 4 September 2023). [30]

Joint Task Force Transformation Initiative (2018), *Risk management framework for information systems and organizations:*, National Institute of Standards and Technology, Gaithersburg, MD, https://doi.org/10.6028/nist.sp.800-37r2. [34]

L'institut Paris Region (2023), *Paris Region Facts and Figures 2023*, https://en.institutparisregion.fr/resources/publications/paris-region-facts-and-figures-2023/ (accessed on 4 September 2023). [41]

Manca, F. (2023), "Six questions about the demand for artificial intelligence skills in labour markets"*, OECD Social, Employment and Migration Working Papers*, No. 286, OECD Publishing, Paris, https://doi.org/10.1787/ac1bebf0-en. [58]

Microsoft (2022), *Regular Expression Language - Quick Reference*, https://learn.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference (accessed on 4 April 2023). [57]

Ministère de l'Enseignement Supérieur et de la Recherche (2023), *État de l'Enseignement supérieur, de la Recherche et de l'Innovation en France n°12 - annexes*, https://publication.enseignementsup-recherche.gouv.fr/eesr/FR/EESR12_Annexe_8/les_niveaux_de_formation/ (accessed on 30 October 2023). [61]

Ministère de l'Enseignement Supérieur et de la Recherche (2021), *Nomenclature relative au niveau de diplôme*, https://www.enseignementsup-recherche.gouv.fr/fr/nomenclature-relative-au-niveau-de-diplome-45785 (accessed on 23 October 2023). [60]

Ministry of Digital Affairs (2019), *Cybersecurity strategy of the Republic of Poland for 2019-2024*, https://digital-skills-jobs.europa.eu/en/actions/national-initiatives/national-strategies/poland-cybersecurity-strategy-republic-poland-2019 (accessed on 4 September 2023). [29]

Ministry of Digital Affairs (2017), *National Framework Of Cybersecurity Policy Of The Republic Of Poland For 2017-2022*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Cybersecuritystrategy_PL.pdf (accessed on 16 November 2023). [31]

NICCS (2023), *Systems Architecture: Security Architect*, https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/systems-architecture (accessed on 14 March 2023). [33]

NICCS (2023), *Workforce Framework for Cybersecurity (NICE Framework)*, https://niccs.cisa.gov/workforce-development/nice-framework (accessed on 5 May 2023). [36]

NICCS (2022), *NICE Cybersecurity Workforce Framework Work Roles*, https://niccs.cisa.gov/workforce-development/nice-framework/work-roles/cyber-defense-analyst (accessed on 5 May 2023). [35]

OECD (2023), *Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. [6]

OECD (2023), *Building a Skilled Cyber Security Workforce in Latin America: Insights from Chile, Colombia and Mexico*, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/9400ab5c-en. [10]

OECD (2023), *OECD*, https://gpseducation.oecd.org/Home (accessed on October 2023). [7]

OECD (2022), *Skills for the Digital Transition: Assessing Recent Trends Using Big Data*, OECD Publishing, Paris, https://doi.org/10.1787/38c36777-en. [9]

OECD (2021), *OECD Economic Surveys: France 2021*, OECD Publishing, Paris, https://doi.org/10.1787/289a0a17-en. [16]

OECD (2021), *OECD Skills Outlook 2021: Learning for Life*, OECD Publishing, Paris, https://doi.org/10.1787/0ae365b4-en. [4]

Pollet, M. (2022), *Cybersécurité : la pénurie de talents risque de « limiter » les efforts de l'Europe*, https://www.euractiv.fr/section/economie/news/cybersecurite-la-penurie-de-talents-risque-de-limiter-les-efforts-de-leurope/?_ga=2.140043636.698086420.1694012923-1631724028.1692711101 (accessed on 18 September 2023). [2]

République Française (2023), *2023, l'année de la maturité pour la qualité de vie en télétravail ?*, https://www.pole-emploi.org/accueil/actualites/2023/2023-lannee-de-la-maturite-pour-la-qualite-de-vie-en-teletravail.html?type=article (accessed on 4 September 2023). [18]

Statistics Poland (2023), *Area and population in the territorial profile in 2023*, https://stat.gov.pl/en/topics/population/population/area-and-population-in-the-territorial-profile-in-2023,4,17.html (accessed on 4 September 2023). [39]

Statistische Ämter des Bundes und der Länder (2023), *Fortschreibung des Bevölkerungsstandes, Code 12411*, https://www.regionalstatistik.de/genesis/online?operation=abruftabelleBearbeiten&levelindex=1&levelid=1693476532184&auswahloperation=abruftabelleAuspraegungAuswaehlen&auswahlverzeichnis=ordnungsstruktur&auswahlziel=werteabruf&code=12411-01-01-5&auswahltex (accessed on 29 September 2023). [40]

Stifterverband (2023), *Forschung Und Entwicklung In Der Wirtschaft 2021*, https://www.stifterverband.org/sites/default/files/2023-04/fue-facts_2021.pdf (accessed on 30 October 2023). [13]

The Local.de (2021), *Germany 'desperately searching' for skilled workers to plug shortage*, https://www.thelocal.de/20210623/germany-desperately-searching-for-skilled-workers-to-plug-shortage (accessed on 30 October 2023). [64]

UNESCO (2018), *International Standard Classification of Education - ISCED 2011*, https://uis.unesco.org/en/topic/international-standard-classification-education-isced (accessed on 20 October 2023). [47]

UNESCO (2017), *ISCED data mapping*, https://isced.uis.unesco.org/data-mapping/ (accessed on 20 October 2023). [62]

UNESCO - UNEVOC (2023), *UNESCO TVETipedia Glossary: Technical Skills*, https://unevoc.unesco.org/home/TVETipedia+Glossary/lang=en/show=term/term=Technical+skills (accessed on 1 March 2023). [8]

Weber, E. and C. Röttger (2021), *No Big Quit in Germany*, https://blogs.lse.ac.uk/covid19/2021/11/24/no-big-quit-in-germany/ (accessed on 19 September 2023). [65]

World Economic Forum (2022), *Global Cybersecurity Outlook 2022*, https://www.weforum.org/reports/global-cybersecurity-outlook-2022/ (accessed on 1 March 2023). [15]

Annex 2.A. Methodological annex

Classifying cyber security job using job titles

The online job postings (OJPs) data provided by Lightcast for European countries are mapped to the International Standard Classifications of Occupations (ISCO-08), a four-digit hierarchical classification used to categorise each OJP in one of the several occupations contained in this structure. However, for the purpose of identifying cyber security job postings, the ISCO-08 lacks granularity. Within the two-digit group "ICT professionals" (25), the four-digit occupation "Database and network professionals not elsewhere classified" (2529) includes occupations performing some tasks related with the cyber security profession, such as "encrypting data transmissions and erecting firewalls", "regulate access to safeguard information" or "performing risk assessments", but it is not limited to this occupation (International Labour Organization, n.d.[56]).

In this context, leveraging the text available in the job titles contributes to obtaining a more precise classification of cyber security job postings. For this purpose, this report uses a classification strategy based on regular expressions. This concept refers to sequences of characters provided to an algorithm to match patterns in a text (Microsoft, 2022[57]).

The first four rows in Annex Table 2.A.1 show the regular expressions selected for classifying the OJPs. These expressions are firstly based on (OECD, 2023[10]), which, secondly, was complemented evaluating hundreds of the most frequent bigrams (all the possible combinations of two words) extracted from the job titles available in English, French, German and Polish. Thirdly, additional search terms which are representative of the cyber industry in France were added, with their translations into the other three languages. Lastly, for OJPs that matched the regular expression of "(?i)system(?=.*network)" or "(?i)network(?=.*system)", the most highly demanded skills were evaluated per job posting, to see if in that particular case, the job could be viewed as a cyber job. After a manual review of the results for each country, additional expressions were necessary to exclude some jobs misclassified in the first stage, as shown in the second row in Annex Table 2.A.1.

Annex Table 2.A.1. Regular expressions in job titles for classifying cyber security jobs

Regular expressions are sequences of characters used to match a pattern in a text.

<table>
<tr><th>Group</th><th>Regular expressions</th></tr>
<tr><td>English expressions for <b>classifying</b> job postings as cyber security jobs</td><td>"(?i)arcsight", "(?i)cyber.*", "(?i)endpoint", "(?i)fortinet", "(?i)security.*info", "(?i)info.*security", "(?i)application(?=.*security)", "(?i)security(?=.*architect)", "(?i)data(?=.*(protection|security|defence|defense))", "(?i)info(?=.*(protection|defence))", "(?i)infrastructure(?=.*security)", "(?i)network(?=.*(security|defence|defense))", "(?i)security(?=.*(architect|devops|infrastructure|software|develop|programm))", "(?i)IT-security.*engineer", "(?i)security(?=.*(data|infrastructure|network))", "(?i)cryptography","(?i)cryptographie", "(?i)hack", "(?i)pentester", "(?i)firewall", "(?i)penetration", "(?i)malware", "(?i)ransomware", "(?i)incident.*response", "(?i)VPN", "(?i)threat.*intelligence", "(?i)zero-day", "(?i)vulnerability.*assessment", "(?i)cloud.*security", "(?i)ISO 27001", "(?i)GDPR", "(?i)white hat", "(?i)black hat", "(?i)phishing", "(?i)spear phishing", "(?i)CISSP", "(?i)antivirus", "(?i)secure coding", "(?i)encryption", "(?i)zero trust", "(?i)vulnerability management", "(?i)mobile.*security", "(?i)IoT.*security", "(?i)data breach", "(?i)system(?=.*network)", "(?i)network(?=.*system)"</td></tr>
<tr><td>French expressions for <b>classifying</b> job postings as cyber security jobs</td><td>"(?i)s.{0,2}curit.*info", "(?i)info.*s.{0,2}curit", "(?i)s.{0,2}curit.*application", "(?i)application.*s.{0,2}curit", "(?i)(donn.{0,2}es.*|infrastructure.*|r.{0,2}seau).*(s.{0,2}curit|d.{0,2}fense|protection)", "(?i)(s.{0,2}curit|d.{0,2}fense|protection).*(donn.{0,2}es|infrastructure|r.{0,2}seau)", "(?i)(protection|d.{0,2}fense)(?=.*info)", "(?i)info.*(protection|d.{0,2}fense)", "(?i)(architecte|devops|infrastructure|logiciel|d.{0,2}velop|program).*s.{0,2}curit", "(?i)s.{0,2}curit.*(architecte|devops|infrastructure|logiciel|d.{0,2}velop|program)", "(?i)cryptographie", "(?i)pare.feu",</td></tr>
</table>

<table>
<tr><th>Group</th><th>Regular expressions</th></tr>
<tr><td></td><td>"(?i)p.{0,2}n.{0,2}tration", "(?i)test.*intrusion", "(?i)intrusion.*test", "(?i)veille.*menaces", "(?i)menaces.*veille", "(?i)s.{0,2}curit.*terminaux", "(?i)terminaux.*s.{0,2}curit", "(?i)RSSI","(?i)RGPD", "(?i).{0,2}valuation.*vuln.{0,2}rabilit", "(?i)vuln.{0,2}rabilit.*valuation", "(?i)s.{0,2}curit.*cloud", "(?i)cloud.*s.{0,2}curit", "(?i)chapeau blanc", "(?i)chapeau noir", "(?i)codage.*s.{0,2}curis", "(?i)s.{0,2}curis.*Codage", "(?i)chiffrement", "(?i)gestion.*vuln.{0,2}rabilit", "(?i)vuln.{0,2}rabilit.*gestion", "(?i)s.{0,2}curit.*mobile", "(?i)mobile.*s.{0,2}curit", "(?i)s.{0,2}curit.*IoT", "(?i)IoT.*s.{0,2}curit", "(?i)violation.*donn.{0,2}es", "(?i)donn.{0,2}es.*violation", "(?i)r.{0,2}ponse.*incidents", "(?i)incidents.*r.{0,2}ponse", "(?i)syst.{0,2}me(?=.*(r.{0,2}seau))", "(?i)r.{0,2}seau(?=.*(syst.{0,2}me))"</td></tr>
<tr><td>German expressions for <b>classifying</b> job postings as cyber security jobs</td><td>"(?i)sicherheit.*info", "(?i)info.*sicherheit", "(?i)application(?=.*sicherheit)", "(?i)sicherheit.*application", "(?i)(daten|infrastruktur|netzwerk)(?=.*(schutz|sicherheit|verteidigung))", "(?i)(schutz|sicherheit|verteidigung)(?=.*(daten.*|infrastruktur.*|netzwerk))", "(?i)info(?=.*(schutz|verteidigung))", "(?i)(schutz|verteidigung).*info", "(?i)infrastruktur(?=.*sicherheit)", "(?i)sicherheit.*infrastruktur", "(?i)netzwerk(?=.*(sicherheit|verteidigung))", "(?i)(sicherheit|verteidigung)(?=.*netzwerk)", "(?i)sicherheit(?=.*(architekt|devops|infrastruktur|software|entwick|program))", "(?i)(architekt|devops|infrastruktur|software|entwick|program).*sicherheit", "(?i)IT-sicherheit.*ingenieur", "(?i)ingenieur.*IT-sicherheit", "(?i)kryptographie", "(?i)info*.bedrohung","(?i)schwachstellenanalys","cloud*.sicherheit", "(?i)dsgvo", "(?i)sicher*.programmierung","(?i)verschl.{0,2}sselung", "(?i)verwaltung*.schwachstellen", "(?i)mobil.*sicherheit","(?i)iot .*sicherheit", "(?i)datenversto", "(?i)system(?=.*netzwerk)", "(?i)netzwerk(?=.*system)"</td></tr>
<tr><td>Polish expressions for <b>classifying</b> job postings as cyber security jobs</td><td>"(?i)bezpiecze.{0,2}stw.*info", "(?i)info.*bezpiecze.{0,2}stw", "(?i)aplikacj(?=.*bezpiecze.{0,2}stw)", "(?i)bezpiecze.{0,2}stw(?=.*architekt)", "(?i)dan.{0,2}(?=.*(ochron|bezpiecze.{0,2}stw|obron|defens))", "(?i)info(?=.*(ochron|obron))", "(?i)infrastruktur(?=.*bezpiecze.{0,2}stw)", "(?i)sie(?=.*(bezpiecze.{0,2}stw|obron|defens))", "(?i)bezpiecze.{0,2}stw(?=.*(architekt|devops|infrastruktur|oprogramowan|rozw.{0,2}j|programowani))", "(?i)bezpiecze.{0,2}stw(?=.*(dan|infrastruktur|sie))", "(?i)kryptografi", "(?i)zapora sie", "(?i)penetracj", "(?i)z.{0,2}o.{0,2}liwe oprogramowani", "(?i)reagowania na incydenty", "(?i)rozpoznawani.*zagro.{0,2}e", "(?i)ocen.*podatno.{0,2}c", "(?i)bezpiecze.{0,2}stw.*chmur", "\\bRODO\\b", "(?i)antywirus", "(?i)bezpieczne programowani", "(?i)szyfrowani", "(?i)zarz.{0,2}dzanie podatno.{0,2}ciam", "(?i)bezpiecze.{0,2}stw.*mobiln", "(?i)bezpiecze.{0,2}stw.*IoT", "(?i)naruszenie.*dan", "(?i)sie(?=.*(systemow))","(?i)systemow(?=.*(sie))"</td></tr>
<tr><td>Expression for <b>excluding</b> job postings from cyber security jobs</td><td>"(?i)growth.*hack", "(?i)cyber store","(?i)fire", "(?i)civil", "(?i)mechanic", "(?i)electric", "(?i)building", "(?i)mandataire.*protection", "(?i)incendie", "(?i)\\bfeu\\b", "(?i)civil", "(?i)m.{0,2}cani(q|c)", "(?i)lectri(q|c)", "b.{0,2}timent", "(?i)feuer", "(?i)brand", "(?i)zivil", "(?i)mechanik", "(?i)elektr", "(?i)\\bbau", "(?i)po.{0,2}aro", "(?i)ogni", "(?i)budow(lan|nictw)", "(?i)mechanik", "(?i)elektr"</td></tr>
</table>

Source: OECD calculations based on Lightcast data.

Groups of roles within the cyber security profession

Within the cyber security OJPs there is a variety of roles demanded by enterprises. Identifying these roles can be useful to characterise cyber security job markets with more detail than traditional labour markets' data sources. Specifically, job titles are once again a rich source of information useful to extract this feature. This report uses an approach based on keywords matches to classify each online job posting in a given role.

Based on (OECD, 2023[6]) and (OECD, 2023[10]), four groups of roles are considered: analysts, architects and engineers, auditors and advisors, and managers. The approach assigns different keywords to each group that allows the algorithm to classify each OJP in the appropriate role. Annex Table 2.A.2 shows the keywords selected for each group, as well as a sample of the job titles classified on each of them. If not classified in one of the groups, job postings are assigned to the category "others".

Annex Table 2.A.2. Groups of cyber security roles

Cyber security groups	Keywords	Sample of job titles
Analysts	analyst, officer, expert, professional, associate, Spezialist, beauftragter, sp.{0,2}cialist, officier, professionnel, associé, analityk, oficer, ekspert, specjalista	Information Security Analyst , Cyber Security Analyst
Architects and engineers	Engineer, architect, technician, developer, devops, tester, administrator, admin, impl.{0,2}ment, Ingenieur, Architekt, Techniker, Entwickler, DevOps, Verwalter, informatiker, ingenieur, technicien, d.{0,2}veloppeur, p.{0,2}n.{0,2}tration, testeur, administrateur, in.{0,2}ynier, architekt, technik, program, Wdro.{0,2}eniowiec	Cyber Security Engineer, Network Security Engineer
Auditors and advisors	auditor, consultant, counsel, advisor, legal, Berater, anwalt, jurist, recht, revisor, pr.{0,2}fer, auditeur, conseiller, juridique, rewident, konsultant, doradca, prawnik	Network Security Advisor, Cyber Security Senior Consultant
Managers	manager, lead, director, executive, chief, partner, head, coordinator, Gesch.{0,2}ftsf.{0,2}hrer, Leiter, F.{0,2}hrung, koordinator, pr.{0,2}sident, gestionnaire, chef, directeur, ex.{0,2}cutif, partenaire, responsable, kierownik, dyrektor, szef, przewodnicz.{0,2}cy	Information Security Manager, Data Protection Service Operations Manager

Source: OECD calculations based on Lightcast data.

A semantic analysis approach to assess skills relevance

Recent developments in Natural Language Processing (NLP) are useful to leverage the semantic meaning of the information contained in the OJPs. Specifically, a word embedding approach is applied to generate a semantic representation of each word in an *n*-dimensional vector, where each dimension indicates a specific context item. This representation allows for the calculation of mathematical similarity measures to represent the similarity between different skills and professions/occupations. In particular, the approach taken in this report leverages 'Word2Vec', an NLP algorithm developed in 2013 by researchers in Google.

To obtain the most relevant skills for cyber security professionals, the analysis in this report creates a Semantic Skill Bundle Matrix (SSBM) by calculating the cosine similarity index between all possible combinations of skills and professions. The cosine similarity index is based on the cosine of the angle between vector representations of words. When a pair of words are closely related, the angle of their vectors is closed to 0 and the cosine is close to 1. Conversely, when the cosine is negative the words can be related but are opposite in meaning. Specifically, the calculation of the index for occupation A and skill B is:

$$CosSim(A,B) = \frac{(A \cdot B)}{||A||\,||B||}$$

Applying this approach is, therefore, possible to assess whether the skill "Excel" is more relevant to the occupation "economist" or to "painter", based on the semantic closeness of these words' meanings extrapolated from millions of job postings. This is used, in turn, to generate indicators of the relevance of technical and professional skills for cyber security professionals based on the language/semantic analysis of the text contained in the OJPs in each country considered.

Recent OECD work (Manca, 2023[58]) validates the assumption by which semantic similarity scores derived from word embeddings can be used as a measure of skills relevance for each occupation. In particular, the report compares the results of the similarity scores with expert constructed scores available in the O*NET database. It shows that correlation between similarity scores and the O*NET values is positive, strong (0.62) and statistically significant across all possible combinations of occupations and skills.

Annex 2.B. Metropolitan cities versus Metropolitan regions

The standard classification of a metropolitan region is a Territorial Level 3 (TL3) region for which more than 50% of its population live in a functional urban area (FUA) of at least 250 000 inhabitants. TL3 regions are smaller territorial regions that together make-up a region at the first administrative tier of subnational government (TL2). In case of France for instance, the TL2 regions are the *régions,* while the TL3 regions *départements*. FUAs consist of cities and their corresponding hinterlands, areas which are close to the cities. (Fadic et al., 2019[59]).

The current report, by contrast, uses even smaller regional areas, which are called metropolitan cities. This level is used to analyse where the demand for cyber security professionals is located. Cities are chosen as a reference point, due to the availability of the data on job postings in the Lightcast datasets. The datasets contain information on the level of "*commune"* in France, "*gemeinde"* in Germany, and "*miasto"* in Poland, but for ease of referencing these are all called cities in the report.

Cities with 250 000 inhabitants or more are designated as metropolitan cities. While metropolitan cities are part of metropolitan regions, a metropolitan region can encompass a larger area. According to the latest census data, there are 139 metropolitan cities in France, including the communes within Greater Paris or the "Métropole du Grand Paris", 63 in Germany, and 11 in Poland, constituting 15%, 22%, and 17.6% of the population, respectively (INSEE, 2023[38]; Statistics Poland, 2023[39]; Statistische Ämter des Bundes und der Länder, 2023[40]).

Annex 2.C. Classifying OJPs posted in 2022 by minimum ISCED level

The data provided by Lightcast include the original text posted online for advertising each vacancy. This piece of data is a valuable source of information that allows researchers to classify OJPs based on different features, such as education, experience, location, among others. In this case, leveraging the text available in the OJPs description contributes to obtaining a more precise and comparable classification of the level of education required in each country.

The approach implemented for classifying OJPs by minimum ISCED[16] level required by employers implies two main steps. First, extracting chunks of text located around words related to education. The objective of this step is to frame the context for text classification and mitigate errors for words that can have different meanings depending on the context. This is the case, for instance, of the word *licence* in French which refers to a degree in the education context but can also be related to IT application licenses that are part of complementary requirements for the position or to tasks and responsibilities named in the job vacancy.

It is important to note that, in the case of France, nearly half of the OJPs posted in 2022 included the expression “BAC+X”. This expression provides a classification relative to the level *baccalauréat,* with X being the years of education required (after receiving the *baccalauréat*) to obtain a diploma (more information is available in Ministère de l'Enseignement Supérieur et de la Recherche (2021[60])). In this case, the X associated with each expression was extracted from the text and mapped to its corresponding ISCED level based on previous mappings made by official institutions (Ministère de l'Enseignement Supérieur et de la Recherche, 2023[61]). When an OJP includes more than one expression, an additional rule was applied to select the lower number extracted from the expressions.

The second step involves looking for specific keywords by country to identify the level of education required. The keywords selected (see Annex Table 2.C.1) are the result of reviewing the ISCED mapping available on the UNESCO web page (UNESCO, 2017[62]) and the chunks of text extracted from the OJPs description. By actively reviewing the text extracted from the job vacancies descriptions, this methodology maintains its data-driven approach allowing the use of words in English, as some of the descriptions in the OJPs were fully written in English, or more colloquial words used by employers, such as “m1” or “mba” or “fh” (referring to the *fachhochschule* in Germany). Additionally, this approach also allows the inclusion of other expressions that can indirectly reflect a minimum level of education. This is the case of *formation supérieure* in France, which can be assumed to signal the need for a qualification above the *baccalauréat.*

Since some OJPs can include different keywords associated with different ISCED levels, the classification starts by identifying those job vacancies including keywords linked to the lowest level (ISCED 3). Once these OJPs are classified, it continues looking for keywords for the next ISCED level (4 or 5) and in the remaining OJPs, and so on. This order ensures that the classification assigned to each OJP corresponds to the lowest level found.

Finally, this approach includes some limitations. Given that the classification relies on a list of keywords, it is possible that some specific words are missing and, therefore, some OJPs can be misclassified or not classified. To mitigate this risk, this approach implied a continuous check of the OJPs without classification looking for new keywords to introduce in the list. Additionally, different variations of the same words were introduced to account for possible mistakes in words with special characters. This is especially important in Poland. In that sense, OJPs not classified in any of the ISCED levels cannot be categorised as if they would not require an education or training qualification. Therefore, they are presented as “not classified”.

Annex Table 2.C.1. Keywords used for mapping OJPs to ISCED levels

List of words used by ISCED level and country

ISCED code	Keywords		
	France	Germany	Poland
3	baccalauréat	abitur, fachabitur, berufsausbildung	high school, matura, wyksztalcenie min. srednie, wyksztalcenie srednie, srednie wyksztalcenie, wyksztalcenie minimum srednie*, srednie zawodowe, technikum
4	-	techniker, fachinformatiker, (ausbildung)	-
5	formation supérieure, formation commerciale supérieure, bts, dut, technicien	-	-
6	bachelor, degree in, licence, dcg, ba	berufsakademie, bachelor, university degree, degree-qualified, informatikstudium, hochschulgrad, engineerinformatiker, abgeschlossenes studium, profilakademischer abschluss, profilhochschulstudium, hochschulstudium, volljurist, ingenieur, datenschutzrechtler, fh, hochschulabschluss, meister, fachhochschule, (engineer, studium)	licencjat, inzynier, engineer, "bachelors", bachelor, degree in, university degree, graduate, stopien uniwersytecki, wyksztalcenie techniczne, wyzsze techniczne,
7	master, école d'ingénieur, ingénieur, école de commerce, post graduate, postgraduate, ecole dingénieurs, m1, m2, ma, dec	diplom, master, ll.m, mba, masterstudium	magister, master in, masters, wyzsze wyksztalcenie, wyksztalcenia wyzszego, wyksztacenie wyzsze, wyksztalcenie wyzsze
8	phd, doctorat	doktorat, phd, promotion,	doktorat, phd, doktor

Note: In Germany, the words *ausbildung, engineer* and *stadium* are in brackets to reflect that they have a meaning in education not always referring to a specific education level. For instance, the word *studium* can refer to a study (as a noun) but also to university studies (bachelor or higher). To mitigate misclassifications, the methodology used these words in the remaining OJPs after classifying those in the ISCED level 8. While "wyksztacenie wysze", "wykształcenie wyższe", "wyksztacenia wyszego", "wykształcenia wyszego", and "wykształcenia wyższego" in Poland translate as "higher education", (and therefore the inferred minimum degree would be bachelor), OECD experts on the Polish educational system suggest that these keywords are more commonly used to refer to a master's degree.
Source: OECD calculations based on UNESCO ISCED mappings and Lightcast data.

Annex 2.D. Leveraging big data to assess the specialisation of digital skill demands in labour markets

When using job postings to examine the influence of certain skills and technologies across labour markets, several previous studies have focused on counting the increase in the frequency with which the terms related to digital technologies have been mentioned across job postings.

Metrics based on the simple count of the frequency of skill mentions are, however, likely to miss whether such an increase has been concentrated in a small number of sectors/occupations or if, instead, technology and skill demands have actually spread across a wide variety of sectors and occupations, truly permeating labour markets.

In order to accurately capture the growth in the influence of cyber security skill demands across the labour market, this chapter uses machine learning techniques applied to the analysis of online job postings (OJPs) to examine to what extent cyber security skills are interconnected with other skills across job vacancies and in employers' recruitment requirements.

A vector representation of skill keywords in a n-dimensional space is used to assess the connections across skills and, as such, the degree by which skills are pervasive in the online job market. The connections between a group of keywords can be represented by a so-called skill graph. In such a graph, the keywords extracted from online vacancies represent the vertices (also called nodes) which can be either connected when both vertices co-occur in a specific job vacancy or disconnected when both vertices never co-occur in the same vacancy.

An adjacency matrix can be built to represent these skill co-occurrences.[17] Whenever a skill co-occurs with another skill in a certain job vacancy, the row corresponding to the skill "A", and the column corresponding to the skill "B" will get the value 1. Note that the adjacency matrix is symmetric, meaning that the co-occurrence between skills is undirected and therefore commutative.

One can use this adjacency matrix to calculate the eigenvector centrality (EVC) for each skill. The power iteration algorithm is used to derive the relativity score for each vertex v in the network. Given a graph G, and adjacency matrix A, the relative centrality score of a certain skill v can be defined as:

$$EVC_v = \frac{1}{\lambda} \sum_{t \in M(v)} EVC_t = \frac{1}{\lambda} \sum_{t \in G} a_{v,t} EVC_t$$

This measure serves as an important indicator for contextual diversity and the importance of certain skills as compared to other skills in the network. In graph theory, the "eigenvector centrality" is a measure that is commonly used to assess the influence of a node in a network or, in other words, to measure the degree of connectedness of a keyword with the rest of words in the text under examination. Originally, these measures were developed by researchers in Google and used in the PageRank algorithm to quantify the importance of the connections among web pages based on the textual information contained in it (Brin and Page, 2012[55]). The same measure can, however, be used to capture the number of connections that a skill keyword has with other skills as well as the 'quality' of those connections, where higher quality connections are those with other skills that are also highly connected to the rest of the skills in the vector space. To only consider skills which have at least some influence, the lowest 10% of skills in terms of EVC in 2022 are removed from the analysis.

The measure of interest is the change in EVC between 2019 and 2022, compared to the average change in EVC across all skills in between those years. This is used in the analysis to measure the degree by which skills have become less influential in the labour market. This measure is computed for each skill keyword analysed in the database of OJPs. A loss of influence of a skill means a decrease of the connections of that particular skill with other skill demands across job postings, hence an indication of how much that skill is being more concentrated in the labour market in a smaller number of OJPs and occupations.

Annex 2.E. Related occupations

Annex Table 2.E.1. Overview of related occupations

Group	Related job name	ISCO codes
1- Computer and data analysts / administrators	Database and network professionals not elsewhere classified	2529
1- Computer and data analysts / administrators	Database designers and administrators	2521
1- Computer and data analysts / administrators	Systems analysts	2511
1- Computer and data analysts / administrators	Systems administrators	2522
1- Computer and data analysts / administrators	Computer network professionals	2523
2-Software developers and programmers	Web and multimedia developers	2513
2-Software developers and programmers	Applications programmers	2514
2-Software developers and programmers	Software developers	2512
2-Software developers and programmers	Software and applications developers and analysts not elsewhere classified	2519
3-ICT technicians	Web technicians	3514
3-ICT technicians	Information and communications technology user support technicians	3512
3-ICT technicians	Information and communications technology operations technicians	3511
3-ICT technicians	Information technology trainers	2356
3-ICT technicians	Computer network and systems technicians	3513
3-ICT technicians	Telecommunications engineering technicians	3522
4- Maths related professions	Mathematicians, actuaries and statisticians	2120
4- Maths related professions	Statistical, mathematical and related associate professionals	3314
4- Maths related professions	Financial and investment advisers	2412
4- Maths related professions	Financial analysts	2413
5- Engineers and technicians	Mechanical engineers	2144
5- Engineers and technicians	Engineering professionals not elsewhere classified	2149
5- Engineers and technicians	Civil engineers	2142
5- Engineers and technicians	Industrial and production engineers	2141
5- Engineers and technicians	Telecommunications engineers	2153
5- Engineers and technicians	Electronics engineers	2152

Notes

[1] https://lightcast.io/.

[2] The five groups consist of different jobs at the four-digit ISCO level, which were chosen because of their affinity with algorithms, digital skills and use of (big) data. For a list of all selected occupations and their groups selected see Annex 2.E.

[3] However, it should be noted that all of these jobs are more likely to be advertised on line than jobs in other occupations as they are high-skill occupations (Cammeraat and Squicciarini, 2021[5]), which means that these shares might be an overrepresentation of the share over the total labour market demand.

[4] A notable difference with the method expressed in (OECD, 2023[10]) is that keywords about the general data protection regulation (GDPR) have been included for every country, leading to a broader classification of jobs as cyber security jobs.

[5] This growth unfolded within a context of fluctuating economic conditions. In particular, while the French GDP decreased significantly (-8%) in 2020 due to the pandemic, it rebounded by 6.8% in 2021 (OECD, 2021[16]). It is worth noting that the implementation of short-time work schemes during the pandemic played a crucial role in safeguarding employment, during this recession in 2020 (OECD, 2021[16]), which means that the employment numbers in France went from increased by 965 000 in 2021 after decreasing by 175 000 in 2020 (INSEE, 2023[63]), despite the steeper drop in GDP.

[6] This is due to the tendency for high-skilled positions to be prominently featured in the digital job market, reflecting the changing landscape of job recruitment practices (Cammeraat and Squicciarini, 2021[5]).

[7] The growth of OJPs in 2020 can partially be attributed to increased shortages in skilled labour during that year, for which decreased immigration from other European countries was a contributing factor (Adăscăliței and Weber, 2021[66]). Inward migration in Germany fell by around 25% in 2020 due travelling restrictions during the pandemic, which led to increased difficulties finding craftspeople, engineers, nurses, care workers, cooks and metal workers (The Local.de, 2021[64]). This diminished number of average monthly OJPs in 2021 was paired by a decrease in unemployment, but research showed that 56% of unemployed that found a job at the end of 2020 and the first two quarters of 2021 returned to their old job (Weber and Röttger, 2021[65]). It is unlikely that these positions were first advertised on line.

[8] It should be noted, however, that the coverage of the OJPs in Poland is less extensive than for Germany and France.

[9] For further details on the methodology, please see Box 2.1 and 0. Figure 2.6 presents the number of OJPs (Panel A) and the shares (Panel B) in the demand of four cyber security roles: analysts, architects and engineers, auditors and advisors, and managers. Following the inclusion of keywords about the general data protection regulation (GDPR), a larger share of auditors and advisor roles are found among the cyber security jobs.

[10] Examples of corresponding French, German and Polish job titles would be: Juriste Conformité - Compliance et RGPD, Juriste Protection des Données Personnelles, Consultant Datenschutz, Volljurist It-Und Datenschutzrecht, and Prawnik w Zespole TMT/IP & Data Protection.

[11] Including the communes within Greater Paris or the “Métropole du Grand Paris”.

[12] For further details on metropolitan cities, please refer to Annex 2.B.

[13] The figure only includes those OJPs for which the location was known, 74% in France, 74.2% in Germany and 80.9% in Poland.

[14] For instance, skills like communication, teamwork, planning, writing, project management, budget management, Excel, leadership and teaching can be seen as transversal, as they are demanded across a diverse set of occupations (OECD, 2021[4]).

[15] The OJPs in the three countries under consideration do not all contain the same cyber security skills. The largest number of cyber skills can be found in Germany, followed by France. In Poland only one explicit cyber security skill is demanded across OJPs.

[16] International Standard Classification of Education. It is the international reference for classifying education programmes and qualifications by levels.

[17] The extracted skill graph forms an undirected acyclic graph, meaning that skills do not co-occur with themselves. As a result, the diagonal of the adjacency matrix is 0.

3 The landscape of cyber security education and training programmes: The case of France

This chapter delves into the provision of cyber security education and training programmes in France. It focuses on examining the characteristics of the education and training programmes that lead to entry-level jobs in the cyber security field. Particular attention is given to strategies and initiatives aimed at diversifying enrolment, especially in bringing more females into cyber security field. The chapter also highlights efforts to increase employers' involvement in the design and delivery of cyber security learning opportunities, and to give visibility to cyber security in education and training programmes.

Introduction

Chapter 2 underscores the robust and increasing demand for cyber security professionals, particularly highlighted in France where the volume of online job postings (OJPs) in this field has surged. This growth is attributed to the expansion of remote work and the broader integration of digital technologies, a trend accelerated by the COVID-19 pandemic. In France, as elsewhere, when the rising demand for cyber security expertise is not matched with an adequate supply of trained professionals, it results in talent shortages that can lead to vulnerabilities and cyber security threats. Such shortages are evident, with gaps in the cyber security workforce presenting significant challenges for the country.

Education and training to develop appropriate cyber security skills are vital to address these shortages and mitigate risks. France has increasingly become a digitised society where cyber security is a priority, including the necessity for a skilled workforce in this domain. The frequency and sophistication of cyberattacks are outpacing the nation's defensive capabilities, reflected in the substantial growth in job postings for cyber security roles over the last decade. However, there is a notable gap in filled positions, signalling an urgent need for effective education and training systems, as well as policies that promote high-quality course offerings to attract a diverse array of learners. Employer engagement in programme design, clarity of career pathways into cyber security, and efforts to make the field more appealing to underrepresented groups, like females, are strategic actions to fill the workforce gap.

Many newcomers (i.e. individuals with no experience or skill in cyber security) to the cyber security field lack formal education in cyber security, often due to limited awareness and availability of targeted training. While many possess degrees in general computer science, specialised cyber security education is less common. To address this gap, young professionals frequently resort to self-study and utilise their professional networks to enhance their skills, underscoring the need for more accessible and known specialised training opportunities in cyber security.

French cyber security education spans from upper secondary levels like Vocational Baccalaureates to higher education, including advanced technician qualifications (Brevet de Technicien Supérieur, BTS) and university programmes like professional bachelor's degrees. Tailored to labour market demands and learner diversity, these programmes also emphasise advanced qualifications like master's degrees, highly valued by employers for cyber security roles. Additionally, France focuses on non-formal education, offering specialised continuing education modules for quick skill development and career transitions.

This chapter provides insights into the landscape of cyber security education and training in France, outlining strategies and policies aimed at expanding supply, fostering diverse participation, and ensuring the delivery of quality training in alignment with labour market needs.

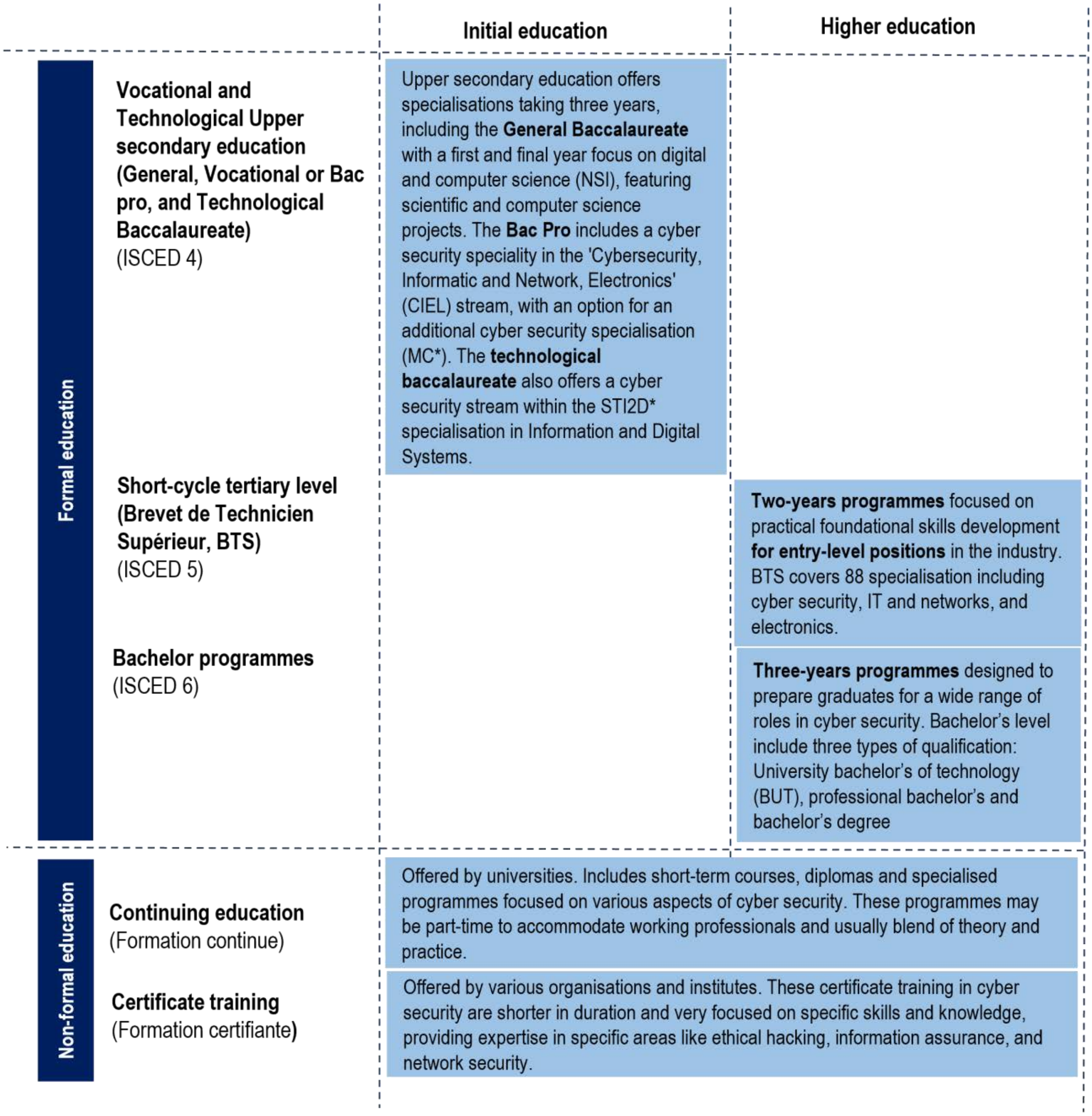
An overview of cyber security education and training in France

This section provides an overview of the education and training landscape to prepare workers for cyber security roles in France. It focuses on education and training programmes that develop cyber security skills for entry-level jobs (i.e. a job that typically does not require advanced level of education and training the field or many years of relevant work experience). The first part of this section describes formal education programmes in this area, starting from vocational upper secondary education and up to master's level programmes. Given the focus on preparation for entry-level jobs, engineering programmes and specialised master's degrees are described here, but are not in the focus of the remaining parts of the report (Box 3.1). Following the description of formal education programmes, the second part of this section looks at non-formal education, which includes courses that do not lead to a formal qualification but may lead to certificates, including those delivered by industry.

Cyber security education and training for entry-level jobs in France include both formal and non-formal programmes. Formal education programmes in cyber security are available at various levels including upper secondary education (Vocational and Technological Baccalaureate), short-cycle tertiary programmes (Brevet de Technicien Supérieur, BTS) and bachelor's level programmes (see Figure 3.1). Much cyber security education and training, however, is offered at the graduate level, involving engineering programmes (leading to an ISCED level 7 qualification) and specialised master's degrees (ISCED level 7). This study focuses on qualifications at or below bachelor's level (ISCED level 6). The programmes covered in this study include both programmes that specifically focus on cyber security and programmes with a slightly broader focus, which include cyber security in their curriculum or as area of specialisation. The latter category includes system engineering, information security, information systems management, ethical hacking, network security and information auditing.

Non-formal education encompasses courses that may lead to certificates but do not confer formal qualifications (see Figure 3.1). Professional certificates are offered by various organisations, providing targeted instruction and practical experience. The recent surge in demand for specialised information and communication technology (ICT) skills, such as cyber security, has led to a notable expansion in other forms of non-formal short courses, such as specialised training modules through continuing education. These offer flexible and accessible learning opportunities, allowing individuals to acquire expertise quickly and efficiently. Focusing on specific skill sets, these courses help address immediate local skill demands (i.e. subregional level) and enable professionals to stay updated with the latest industry developments.

Figure 3.1. An overview of formal and non-formal education programmes that cover the ICT field (including cyber security) in France.



		Initial education	Higher education
Formal education	**Vocational and Technological Upper secondary education (General, Vocational or Bac pro, and Technological Baccalaureate)** (ISCED 4)	Upper secondary education offers specialisations taking three years, including the **General Baccalaureate** with a first and final year focus on digital and computer science (NSI), featuring scientific and computer science projects. The **Bac Pro** includes a cyber security speciality in the 'Cybersecurity, Informatic and Network, Electronics' (CIEL) stream, with an option for an additional cyber security specialisation (MC*). The **technological baccalaureate** also offers a cyber security stream within the STI2D* specialisation in Information and Digital Systems.	
	Short-cycle tertiary level (Brevet de Technicien Supérieur, BTS) (ISCED 5)		**Two-years programmes** focused on practical foundational skills development **for entry-level positions** in the industry. BTS covers 88 specialisation including cyber security, IT and networks, and electronics.
	Bachelor programmes (ISCED 6)		**Three-years programmes** designed to prepare graduates for a wide range of roles in cyber security. Bachelor's level include three types of qualification: University bachelor's of technology (BUT), professional bachelor's and bachelor's degree
Non-formal education	**Continuing education** (Formation continue)	Offered by universities. Includes short-term courses, diplomas and specialised programmes focused on various aspects of cyber security. These programmes may be part-time to accommodate working professionals and usually blend of theory and practice.	
	Certificate training (Formation certifiante**)**	Offered by various organisations and institutes. These certificate training in cyber security are shorter in duration and very focused on specific skills and knowledge, providing expertise in specific areas like ethical hacking, information assurance, and network security.	

Note: STI2D refers to science and technology for industry and sustainable development. MC refers to Mention complémentaire. This figure does not include all forms of non-formal education provided in France.
Source: OECD elaboration based on information from the Ministry of National Education and Youth (Ministère de L'Éducation Nationale et de la Jeunesse, MENJ) and the National Agency of Information Systems Security (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI).

Box 3.1. Defining the scope of cyber security education and training for this case study

In France, cyber security education and training covers a wide range of subjects, catering to varying levels of knowledge and expertise - from basic awareness for the general public to advanced technical training, such as intrusion detection and penetration testing for specialised roles.

This chapter focuses on education and training programmes for entry-level cyber security positions. The National Information Systems Security Agency (ANSSI) is instrumental in shaping the field, setting professional standards, and endorsing certifications. As shown in Table 3.1, entry-level roles in cyber security often do not require substantial work experience or advanced degrees. Therefore, this chapter zeroes in on formal and non-formal training that equips individuals with the essential skills for entry-level roles. Short cycle tertiary (bac+2 or ISCED 5 programmes such as the Brevet de Technicien Supérieur, BTS) and bachelor's level programmes (bac+3 or ISCED 6 programmes such as University Bachelor of Technology, professional and academic bachelor's programmes) are key in broadening access to the profession, promoting diversity, and providing steppingstones towards more advanced education and training. In line with this, the analysis of OJPs reveals higher demand for cyber security professionals with ISCED 5 level qualifications in France compared to Germany and Poland, along with a significant share of ISCED 6 positions (see Chapter 2).

Table 3.1. Minimum level of education and professional experience required in cyber security professions area

Cyber security professions area	Level of education required (Minimum)	Professional experience required (Minimum)	Some occupations, roles
Security management and project management security	Between bac+3 in ICT and bac+5 in cyber security	Between +1 year of relevant experience in the field to +10 years in cyber security field	Cyber security director Head of information system security Security project manager
Design and maintenance of secure information system	Between bac+3 in ICT and bac+5 in cyber security; certifications	Between +1 year of relevant experience in the field to +5 years in cyber security field	Project security manager Security architect Security development specialist Cryptologist Technical security auditor
Security incident and crisis management	Between bac+3 in cyber security and bac+5 in cyber security or system network	Between +1 year and +5 years of relevant experience	Head of the security operation center Head of computer security incident response team (CSRIT) Security Incident response analyst
Advice, services and research	Between bac+3 in cyber security or computer science and bac+5 in cyber security	Between +1 year and +5 years of relevant experience	Cyber security consultant Cyber security trainer Security solutions integrator Information systems security researcher

Source: ANSSI (2020[1]), Panorama des métiers de la cybersécurité, édition 2020, www.ssi.gouv.fr/uploads/2021/10/anssi-panorama_metiers_cybersecurite-2020.pdf.

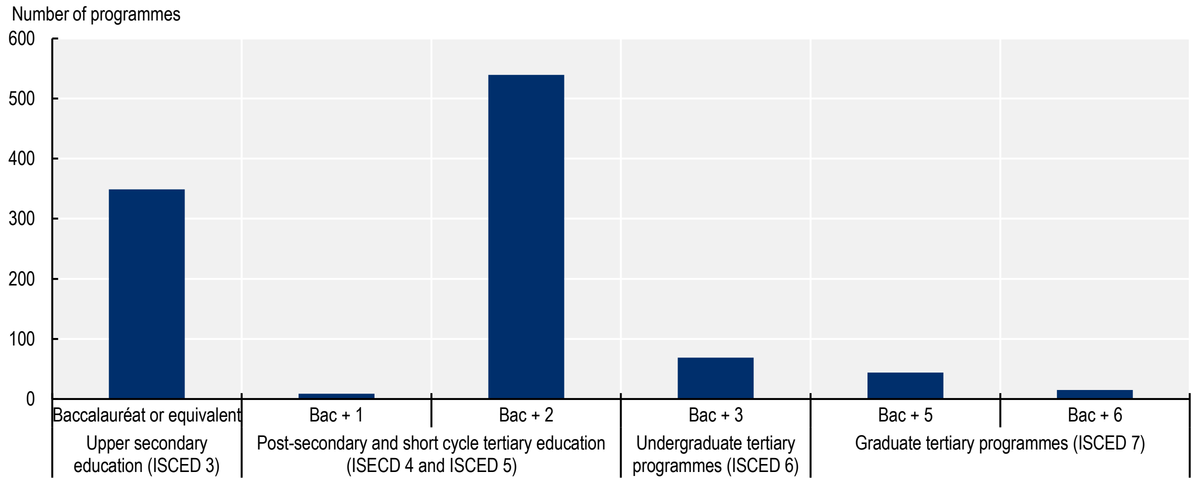
However, compared to other OECD countries in France, master's level programmes (bac+5 or ISCED 7 programmes) in cyber security play a crucial role in equipping individuals with the skills needed to meet the minimum requirements for most technical roles in the sector (see Chapter 2). Thus, there are various training routes available for those seeking more specialised and advanced education in cyber security (ANSSI, 2021[2]). Advanced training plans to become more flexible to learners need and responsive to labour market requirements without compromising the quality and depth of the technical content necessary to prepare highly-skilled cyber security professionals (Gouvernement, 2023[3]).

Formal education programmes

Formal education programmes that develop skills for cyber security are delivered at various levels in France. Among programmes that prepare for a first entry into the labour market, provision ranges from upper secondary programmes (at ISCED level 3) to engineering degrees (at ISCED level 7). This section describes programmes at each level.

The array of formal specialised cyber security programmes is extensive and predominantly focused on short cycle tertiary education (ISCED 4 and 5). For the 2022-2023 academic year, a total of 1 025 cyber security programmes were offered across formal education institutions. The majority of these – around 900 (or 87% of the total) – were concentrated at the upper secondary (ISCED 3) and short-cycle tertiary levels (bac+2, ISCED 5) (see Figure 3.2). A further 69 specialised programmes were available at the bachelor's level (bac+3, ISCED 6). It's important to note that these figures exclude engineering programmes that may incorporate cyber security modules or emphasis, suggesting that the actual number of programmes in this field could be even higher.

Figure 3.2. Number of cyber security programmes by level of education, 2022-2023



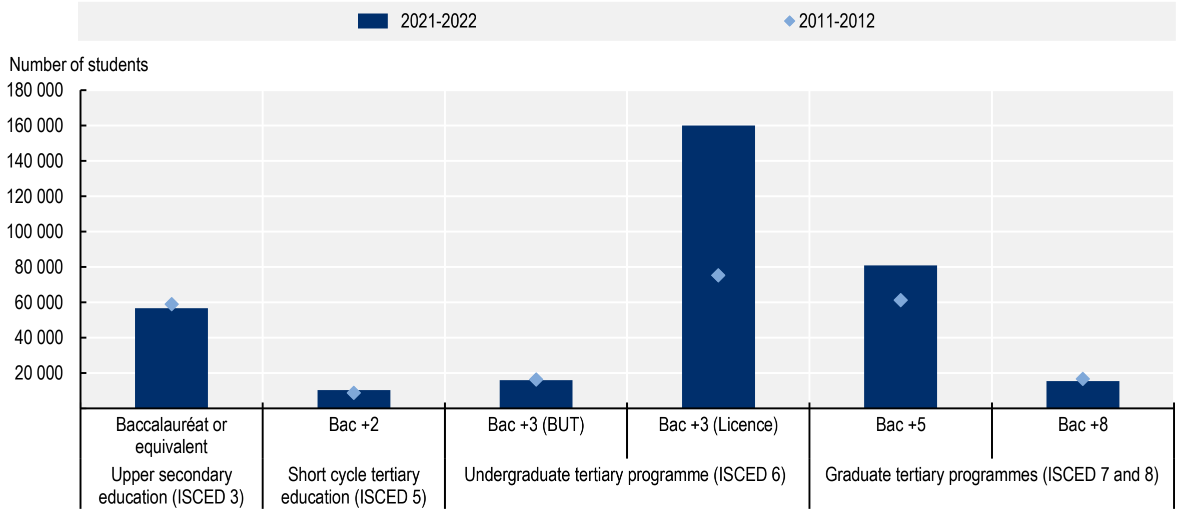
Note: One programme with the same title offered in two institutions is considered two separate programmes, since the interest is to identify the total number of programmes available. Post-secondary and short-cycle tertiary education include a Professional Baccalaureate with an additional mention or supplemental speciality (Mention complémentaire, MC) and a higher technician programme (Brevet de Technicien Supérieur, BTS). Undergraduate tertiary programmes include university bachelors of technology (Bachelors universitaires de technologie, BUT) and the professional bachelor's (Licence professionelle).
Source: ONISEP (2023[4]), L'offre de formations de cybersécurité, www.onisep.fr/

Enrolment in computer science and related areas is considerably concentrated in higher education programmes. In 2021, around 240 000 students in this field enrolled in undergraduate (ISCED 6) and master's (ISCED 7) programmes, marking a 76% increase compared to 2011 (see Figure 3.3). This increase is the result of efforts made by the government to guide young people towards science, technology, engineering and mathematics (STEM) subjects, particularly those programmes that meet the immediate needs of the labour market. In vocational and professional secondary education (ISCED 3), the number of students enrolled in computer science-related programmes has remained stable over the last decade, with approximately 60 000 students.

Even though the number of programmes in short-cycle tertiary education in computer science (e.g. Advanced technician qualifications, Brevet de technician supérieur, BTS in ISCED 5) is higher than in other educational levels, enrolment concentrates in higher education programmes (e.g. University

Bachelor of Technology, professional and academic bachelor's programmes, bachelors in ISCED 6). This can be attributed, on one hand, to recent reforms that have revitalised the offering of courses, particularly in cyber security, computers and networks, and electronics (JORF, 2020[5]) (MESR, 2023[6]), to which enrolment has not yet fully responded. These reforms have introduced more up-to-date content, advanced teaching methodologies, and industry-relevant skills into the curriculum. On the other hand, according to stakeholders interviewed, young people interested in studying computer science tend to enrol in higher education programmes (e.g. bachelor's programmes) due to their potential for career progression. Such programmes often open up more career options, including the possibility of academic research or more specialised roles, and offer greater global recognition.

Figure 3.3. Number of students enrolled in computer sciences by level of education, 2021-2022



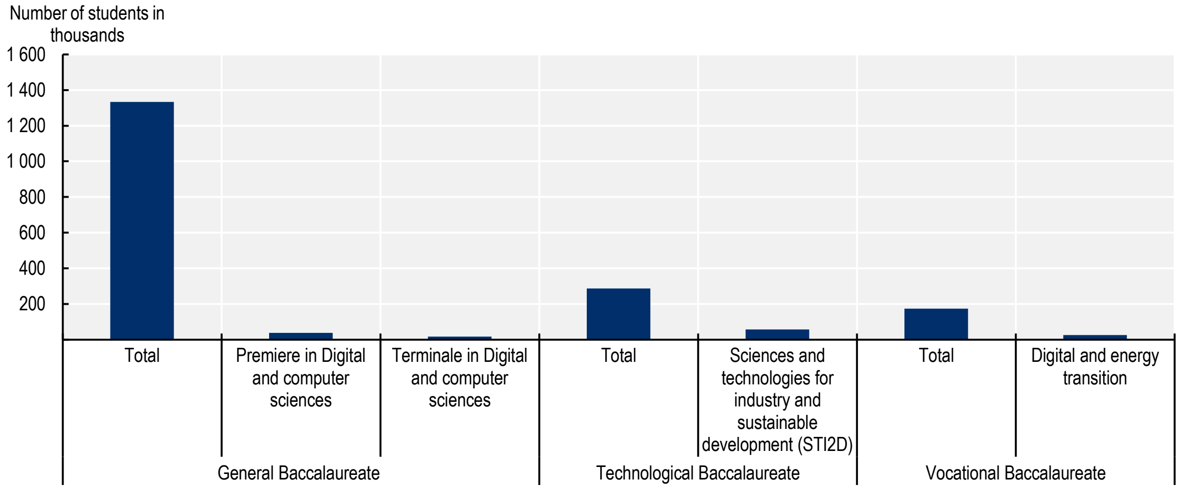
Note: These figures include students enrolled in computer sciences and related fields, including cyber security. Baccalauréat includes students enrolled in vocational baccalauréat in the Science and Technology for Industry and Development (STI2D). Short cycle tertiary education includes Brevet Technicien Supérieur programmes (BTS) in computer sciences and computing, information processing and data management. Undergraduate programmes include Bachelor Universitaire de Technologie (BUT), professional bachelor and bachelor programmes in applied sciences, computer sciences. electrical engineering and related fields.
Source: Depp (2022[7]), Repères et références statisques sur les enseignements, la formation et la recherche 2022, www.education.gouv.fr/media/116557/download; Depp (2012[8]), Repères et références statisques sur les enseignements, la formation et la recherche, 2012, https://cache.media.enseignementsup-recherche.gouv.fr/file/2012/06/4/DEPP-RERS-2012_224064.pdf.

Upper secondary level

In France, upper secondary education leads to three types of baccalaureate qualifications (qualification delivered in upper-secondary education in France): the General, Technological and Vocational Baccalaureate. All three programmes take three years to complete and serve both as an upper-secondary education diploma and as a university entrance exam. Depending on the specialisation and optional subjects chosen, students are tested on a broad range of topics. The results are critical for admission into higher educational institutions, including universities, Grandes Écoles, and technical institutes.

Most students opt for the General Baccalaureate option in upper-secondary education. However, among those in General Baccalaureate, only few choose to take classes related to computer sciences and digital technology, which can be relevant for pursuing more advanced education in the field of cyber security. In 2021, only 54 000 General Baccalaureate students, including those in their second and third years of upper secondary education, took classes in this area of knowledge (4% of all General Baccalaureate students) (see Figure 3.4). Nevertheless, this proportion has grown compared to 2011, showing a 30% increase.

Figure 3.4. Total number of students and number of students in fields related to computer sciences by type of baccalaureate qualifications, in 2021



Note: For General Baccalaureate only students choosing subjects related to computer sciences such mathematics, Digital and computer science, physics and chemistry are considered. In the French education system, “première” and “terminale” are the final two years of the General Baccalaureate programme. “Première” is equivalent to the junior year of high school, and “terminale” corresponds to the senior year. During these years, students typically focus on more specialised subjects in preparation for the baccalaureate exams, which are crucial for university admission in France.

Source: DEPP (2023[9]), Repères et références statistiques, edition 2023, www.education.gouv.fr/reperes-et-references-statistiques-2023-378608.

Enrolment in cyber security relevant fields in Technological and Professional Baccalaureate is higher than in General Baccalaureate, which indicates learners in these programmes are interested in getting skills needed for immediate employment upon graduation, since they are involved in more hands-on training and have stronger ties to the industry. More than 20% of students of Technological Baccalaureate are enrolled in the Science and Technologies for Industry and Sustainable Development (STI2D) programme including cyber security training. A similar proportion (17%) of students in Professional Baccalaureate are enrolled in the digital and energy transition programme. These shares have increased over time (12 percentage points and 17 percentage points. compared to 2018) reflecting an increase in the interest of learners in engaging in training in related to the ICT sector. The following sections will discuss in more detail the last two programmes: Vocational and Technological Baccalaureate.

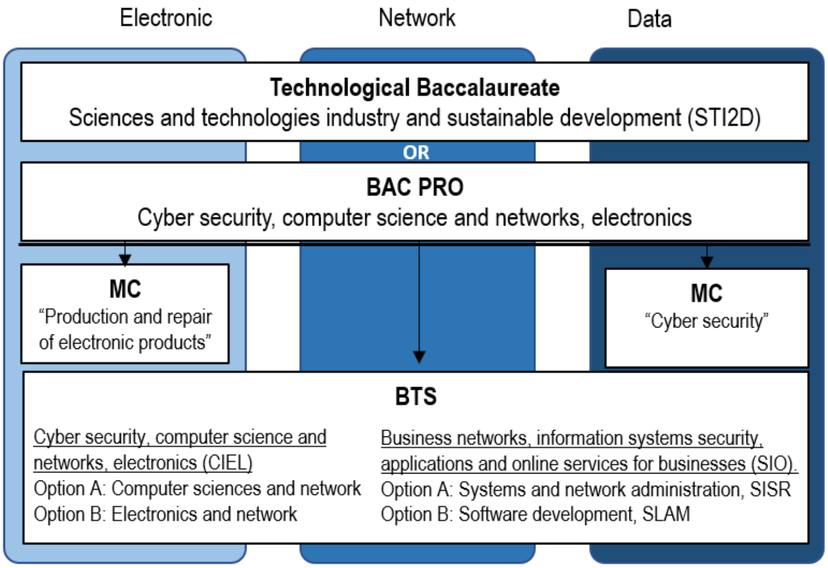
Vocational Baccalaureate

The Vocational Baccalaureate (baccalaureate professionnel, bac pro) prepares students for a specific profession, but also allows for the possibility of further studies, especially for technical higher education courses such as BUT. These courses are offered by vocational upper secondary schools (*lycées professionnels*) and cover a range of professional fields including information technology (IT). One of the programmes is entitled “Cyber security, IT, networks and electronics”, offered within the “digital and energy transition” professional family. Over the three years of the programme, students gradually specialise within a field and towards a selected profession. Students who pursue a school-based route first spend their first year focusing on “Professions of the digital and energy transitions” and may chose cyber security during the second year. Alternatively, students may pursue the programme through an apprenticeship (whereby students alternate education and training in schools and in companies), starting in the first year with a focus on cyber security. Programmes are designed to lead into the labour market, as technicians. It is however possible, subject to certain conditions outlined below, to access a higher education programme.

Upon completing a bac pro, students have several pathways available to them, both in terms of further education and immediate job opportunities. They might choose to further their studies through programmes such as the BTS, a two-year course aligned with their field. Alternatively, some may venture directly into university aiming for bachelor's or master's degrees in relevant subjects or even explore non-formal training providers offering courses in cyber security. In terms of immediate employment, the bac pro qualification makes them eligible for entry-level roles in cyber security, ranging from junior analyst positions to IT support roles with a security emphasis. Internships are another viable route, providing hands-on experience and potential full-time job offers.

From the start of the 2023 academic year, bac pro programmes offered in the field of "digital system" become "Cyber security, computer sciences and networks, electronics, (Cybersécurité, Informatique, et réseaux, electronique, CIEL" (see Figure 3.5) (MENJ, 2023[10]). Following this reform (JORF, 2023[11]), learners interested to engage with further education will have two options after completing a bac pro in CIEL: (1) Engaging directly with a BTS in CIEL and specialised either in "Computer sciences and network" or in "Electronics and network", or (2) engaging with an extra year to obtain a field specialisation (Mention complémentaire or MC) either in "Production and repair of electronic products" or in "cyber security". This additional year for field specialisation is designed to provide specialised skills or knowledge in a specific field, complementing the education and training received in the initial course of study (MENJ, 2023[12]). A MC includes both classroom instruction and practice-oriented vocational training through internships. The goal is to deepen students' skills in a particular area, making them more competitive in the job market or preparing them for further studies.

Figure 3.5. Pathways into cyber security skills in vocational baccalaureate education

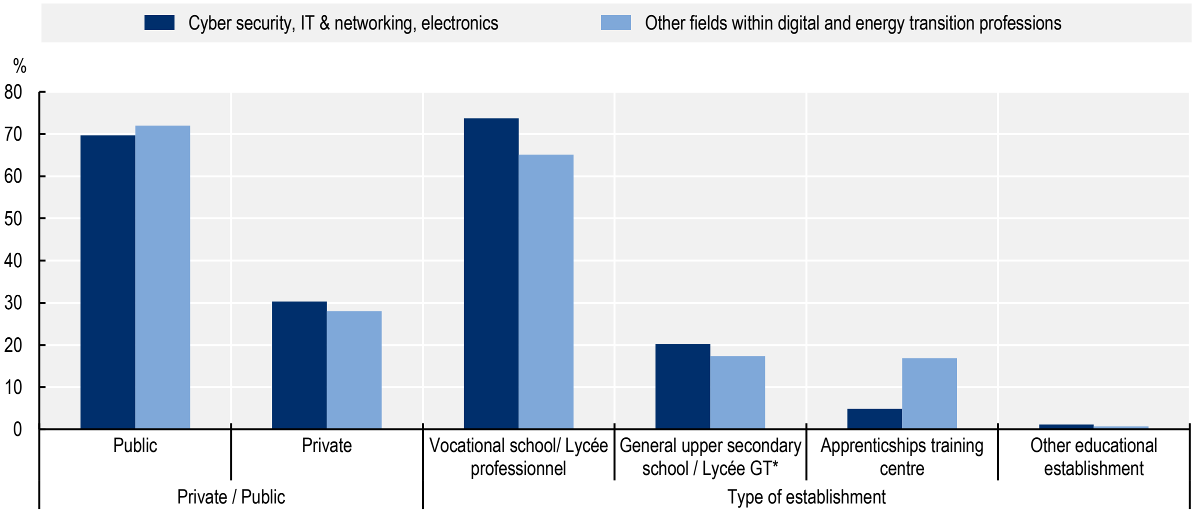

Electronic
Network
Data
Technological Baccalaureate
Sciences and technologies industry and sustainable development (STI2D)
OR
BAC PRO
Cyber security, computer science and networks, electronics
MC
"Production and repair of electronic products"
MC
"Cyber security"
BTS
Cyber security, computer science and networks, electronics (CIEL)
Option A: Computer sciences and network
Option B: Electronics and network
Business networks, information systems security, applications and online services for businesses (SIO).
Option A: Systems and network administration, SISR
Option B: Software development, SLAM

Note: BTS refers to Brevet de Technicien Supérieur. MC refers to Mention complémentaire.
Source: ONISEP (2023[13]), Bac pro cybersécurité, informatique et réseaux, électronique (CIEL), www.onisep.fr/ressources/univers-formation/formations/Lycees/bac-pro-cybersecurite-informatique-et-reseaux-electronique, EDUSCOL (2023[14]), Rénovation de la filière systèmes numériques en "Cybersécurité, Informatique et réseaux, Electronique (CIEL) ", https://eduscol.education.fr/sti/actualites/renovation_filiere_ciel.

The CIEL Vocational Baccalaureate trains technicians who can intervene in the production and maintenance processes of electronic products (production of models and prototypes, maintenance of an electronic system or computer network). Students acquire the skills to implement computer networks (installation of the elements of an electronic system and operation of the network). They are also trained in the analysis of software or hardware, for the purpose of cyber security and data enhancement. Graduates are trained to carry out activities in the “4.0” industry, in the fields of intelligent networks and data exploitation: industry (industrial automation, “4.0 and 5.0” factories, smart city, etc.), home automation, cyber security, telemedicine and health, transport, telecommunications, the Internet of things, etc.

Cyber security, IT and network vocational programmes are predominantly offered by upper secondary vocational schools (*Lycée professionnel*) compared to other programmes within the digital and energy transition field (see Figure 3.6). The predominance of bac pro in cyber security at *Lycée professionnel* institutions implies a strong emphasis on practical, job-ready skills closely aligned with industry needs. While this makes the training accessible and directly applicable to the workforce, it may lack the theoretical depth and broader academic context often required by university-level courses. This focus on vocational training is valuable for immediate employability especially for entry level jobs. However, given most cyber security roles require higher level qualifications and deeper expertise in the cyber security field, bac pro graduates are likely to need additional training in further education to develop skills allowing them to progress to more advanced job positions.

Figure 3.6. Distribution of vocational baccalaureate programmes in cyber security, IT and networks, and electronics and other digital and energy transition fields, by type of establishment in 2023



Note: Other educational establishment also includes rural family home, regional adapted education establishment and college. Lycée GT refers to General and Technological Upper Secondary School (*Lycée General et Technologique*).
Source: ONISEP (2023[15]) Les familles de métiers en seconde professionnelle, www.onisep.fr/formation/apres-la-3-la-voie-professionnelle/les-diplomes-de-la-voie-pro/le-bac-professionnel/les-familles-de-metiers.

Technological Baccalaureate

The Technological Baccalaureate is designed to provide students with foundational knowledge in specific technological fields such as engineering sciences, IT, health sciences, and agronomy. Unlike the academically focused General Baccalaureate, it melds traditional subjects with specialised, career-ready training, particularly in the final two years of upper-secondary education, the “*première*" and “*terminale*”. While the Technological Baccalaureate strikes a balance between academic and technical proficiency in specialised areas, the Vocational Baccalaureate is distinctly designed for students targeting immediate employment, offering hands-on skills, tailored to specific industries.

Students can choose among eight possible programmes covering topics from health and social science to industry, innovation and digital transformation (Education, 2023[16]). Two of the specialisation offered are relevant to the IT and cyber security sector: 'Science and technologies of management' '(*Sciences et technologies du management et de la gestion*, STMG) and Science and technology for industry and sustainable development' (*sciences et technologies de l'industrie et du développement durable*, STI2D) (see Table 3.2). Both programmes include specialties relevant for the cyber security sector. The STMG programme includes a specialisation on 'Information and management systems' which covers the use of information systems and ICT management. The STDI2 programme includes the specialisation 'Information and digital system' which is oriented for students interested in learning how to process digital information and developing hardware and software products, which can be a better fit for learners interested in engaging with more specialised technical education in the cyber security field.

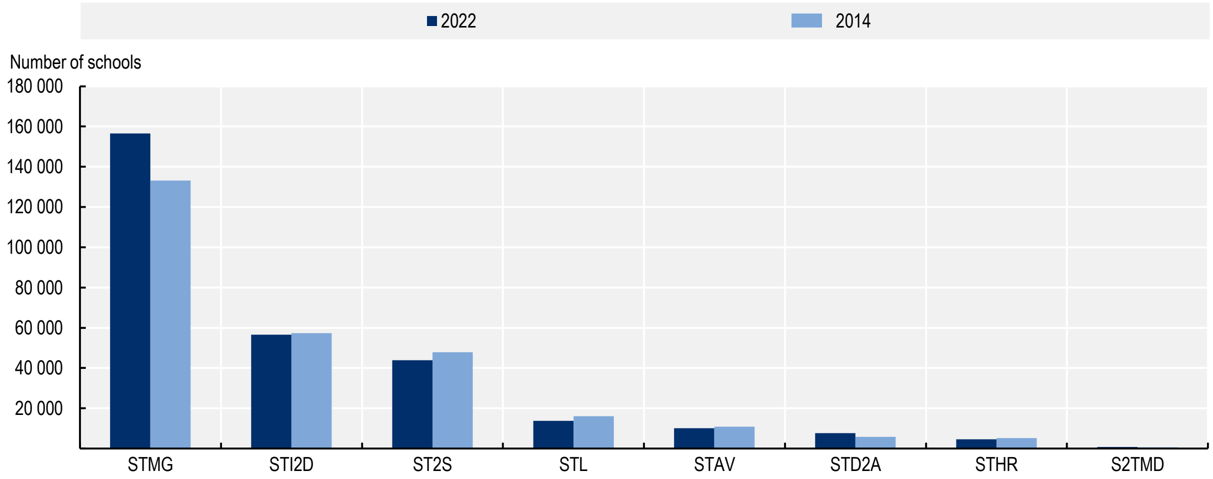
Table 3.2. Technological baccalaureate programmes oriented to ICT, information systems and cyber security

	Description	Specialties	Career prospects
Science and technologies of management (STMG)	This programme is oriented towards students interested in the reality of how organisations operate, relationships at work, new digital uses, marketing and performance measurement, decision analysis and the impact of business strategies.	• Management and finance • Marketing • Human resources and communication • **Information and management systems**	This programme prepares students for careers in finance, management control, information systems, human resources, marketing and communication
Science and technology for industry and sustainable development (STI2D)	This programme is aimed at high school students interested in technological innovation and energy transition, as well as for those that want to understand how technical systems in industry and everyday life work	• Architecture and construction (AC) • Energy and environment (EE) • Technological innovation and eco-design (ITEC) • **Information and digital system (SIN)**	This programme leads to jobs as technicians or engineers in electrical engineering, electronics, IT, mechanics, civil engineering, logistics

Note: Specialties in bold are directly related to the cyber security field.
Source: MENJ (2023[17]), Réussir au Lycée, www.education.gouv.fr/reussir-au-lycee/le-baccalaureat-technologique-1916; ONISEP (2023[18]), Le bac STMG (sciences et technologies du management et de la gestion), www.onisep.fr/formation/apres-la-3-la-voie-generale-et-technologique/qu-est-ce-que-la-voie-generale-et-technologique/la-voie-technologique-en-premiere-et-terminale/le-bac-stmg-sciences-et-technologies-du-management-et-de-la-gestion.

While fewer students overall enrol in the Technological Baccalaureate compared to General Baccalaureate, those who do choose this path are increasingly interested in the offerings of the STI2D programme. Technological Baccalaureate enrolment has decreased in the last decade, especially in the STI2D programme (see Figure 3.7). In 2022, 56 636 students enrolled in STI2D, 748 less than in 2014. However, the share of students in Technological Baccalaureate engaging with STI2D has increased going from 16% in 2014 to 19% in 2022. The STI2D programme resonates with contemporary global challenges and job market trends beyond the cyber security sector. As technological advancements and sustainability become central themes in modern industries, students may perceive STI2D as offering more relevant skills and better future career opportunities.

Figure 3.7. Evolution of enrolment in technological baccalaureate between 2014-2022, by programme specialisation



Note: STMG refers to science and technologies of management. SDT2A refers to science and technology of design and applied arts, STI2D refers to science and technology for industry and sustainable development, STL refers to laboratory science and technology, ST2S refers to health and social sciences and technologies, S2TMD refers to Technical Baccalaureate of music and dance, STHR refers to science and technology in the hotel and restaurant industry, and STAV refers to sciences and technologies of agronomy and living organism.
Source: ONISEP (2022[19]), La voie technologique en première et terminale, www.onisep.fr/formation/apres-la-3-la-voie-generale-et-technologique/qu-est-ce-que-la-voie-generale-et-technologique/la-voie-technologique-en-premiere-et-terminale.

While the Technological Baccalaureate equips students with technical and foundational applied skills, for specialised domains like cyber security, the knowledge and skills garnered through this qualification alone might be insufficient for many entry-level positions. This may be due to the lack of practical skills which makes the Vocational Baccalaureate better placed for initial roles. To delve deeper into cyber security, students typically continue their education at the University Institutes of Technology (Instituts Universitaires de Technologie, IUTs) or other higher technical institutions. Additionally, they can pursue studies at universities or other higher education institutions such as Grandes Écoles. For the latter, students from both Technological and General Baccalaureate who are interested in advanced cyber security learning, such as a bachelor's degree, often enrol in classes prépas. These are preparatory courses designed to ready students for entry into Grandes Écoles (see Box 3.2).

Box 3.2. The General Baccalaureate and classes préparatoire: An additional pathway to access cyber security programmes

In France, the Baccalaureate Général, much like its technologique and professionelle counterparts, offers a foundational step towards a cyber security career. This baccalaureate furnishes students with theoretical training, positioning them for higher education avenues such as the preparatory class (classe préparatoire) or university. Following the 2018 reform, schools deliver a common core curriculum, allowing students to select specialised subjects aligned with their ambitions. Picking subjects like mathematics, physics, and computer science strategically positions students for advanced studies in cyber security, be it in computer science, information technology, or dedicated cyber security programmes.

Preparatory class (Classes Préparatoires aux Grandes Écoles, CPGE)

Classes Préparatoires or classes prépa act as a pivotal bridge for students aspiring to delve deep into cyber security. Focused programmes like MPSI (Mathematics, Physics, and Engineering Sciences) and PCSI (Physics, Chemistry, and Engineering Sciences) provide an intensive grounding in key subjects like mathematics and computer science-foundations vital for grasping cyber security intricacies, from encryption algorithms to network design. Moreover, Classes Prépas prime students for Grandes Écoles, institutions that offer specialised training in several fields, including cyber security. Within these premier schools, students gain advanced technical expertise, while also exploring the ethical, managerial, and societal facets of cyber security. Thus, the rigorous foundation set by Classes Prépas significantly elevates a student's readiness for elite cyber security education.

Source: MENJS (2023[20]), Reussir au Lyceé, www.education.gouv.fr/reussir-au-lycee/le-baccalaureat-technologique-1916.

Short-cycle tertiary level

Advanced technician qualifications (Brevet de technicien supérieur or BTS) are short-cycle tertiary qualifications (ISCED level 5) and take two years to complete. To enrol in a BTS programme, students must hold a baccalaureate. Depending on the specific BTS course, certain types of baccalaureates may be preferred (see Table 3.3).

Table 3.3. Education requirements to access to BTS CIEL

	BTS cyber security, IT and networks, electronics option A IT and networks (CIEL IR)	BTS cyber security, IT and networks, electronics option B electronics and networks (CIEL ER)
General bacclauréate	General Baccalaureate with a scientific orientation	General Baccalaureate with a scientific orientation
Vocational baccalauréate	Professional Baccalaureate in cyber security, IT and networks, electronics	Bac pro agroequipment
		Professional Baccalaureate in cyber security, IT and networks, electronics
	Professional Baccalaureate Electricity professions and its connected environments	Professional Baccalaureate Maintenance of equipment option A agricultural equipment
		Professional Baccalaureate Electricity professions and its connected environments
Technological baccalauréate	Bac techno STI2D sciences and technologies of industry and sustainable development specific teaching information and digital systems	Bac techno STI2D sciences and technologies of industry and sustainable development specific teaching information and digital systems

Source: ONISEP (2023[21]), BTS cybersécurité, informatique et réseaux, électronique option B électronique et réseaux (CIEL ER), www.onisep.fr/ressources/univers-formation/formations/Post-bac/bts-cybersecurite-informatique-et-reseaux-electronique-option-b-electronique-et-reseaux.

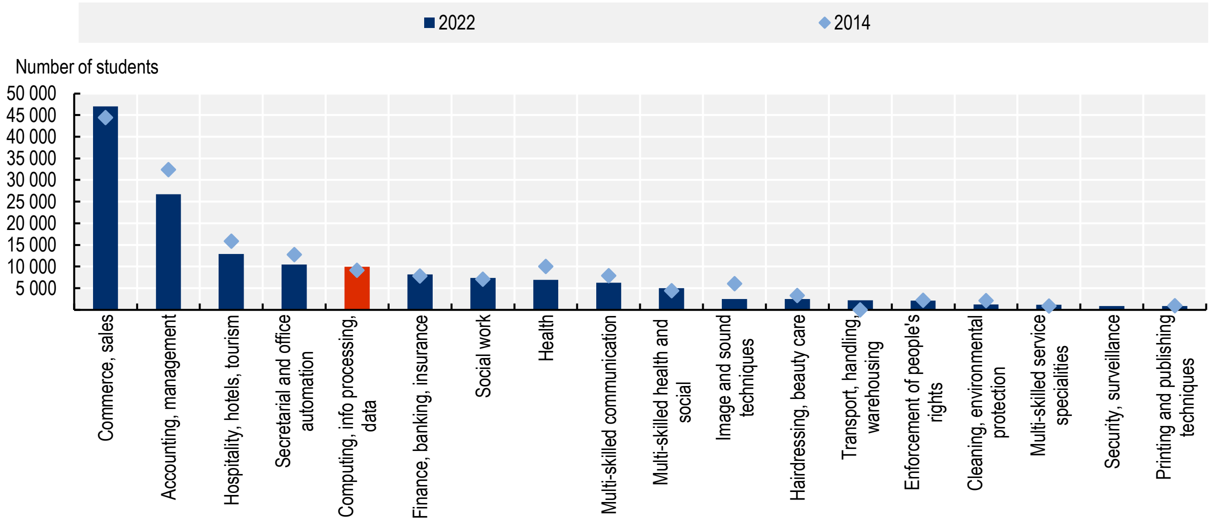
BTS programmes offer specialised vocational training across various fields, blending theoretical lessons with practical experience, often integrating internships. From the 88 available specialisations spanning multiple sectors, students keen on cyber security can select the "IT and Networks, Electronics (cybersécurité, informatique et réseaux, électronique, BTS CIEL)" track. Within this track, two options exist: Option A "Computer science and networks", focusing on training technicians in coding IT solutions, data management, and secure database storage; and Option B "Electronics and networks", emphasising electronic system design, hardware-software assembly, and computer network management (MESR, 2023[22]). While the BTS diploma is fundamentally designed for immediate professional integration, students with commendable academic achievements or exceptional exam marks can advance to a bachelor's degree in Computer Methods Applied to Business Management (MIAGE). Alternatively, they may pursue a professional license in the IT and networks sector, either through an IT-specialised school or a post-baccalaureate in the industrial technology preparatory class (Classes Préparatoire Adaptation Technicien Supérieur, ATS), setting them on track for an engineering school.

After completing a Vocational or Technological Baccalaureate in CIEL or STI2D, students can enroll in the BTS SIO programme (Brevet de Technicien Supérieur – Services Informatiques aux Organisations). Established in 2011, the BTS SIO is a two-year programme recognised by the French state. It prepares graduates for immediate employment in the IT sector or for further studies in computer science. The BTS SIO offers two specialisations: SLAM (Solutions Logicielles et Applications Métiers) and SISR (Solutions d'Infrastructure, Systèmes et Réseaux). SLAM focuses on software solutions and business applications, including drafting specifications, developing software solutions, and integrating them into organisations (Onisep, 2023[23]). SISR targets future professionals in network and computer equipment, emphasising installation, maintenance, and security of IT systems (Onisep, 2023[24]).

Enrolment in short-cycle tertiary programmes has declined over the past decade. However, participation in courses related to computing, information processing, and data management has seen a slight uptick (see Figure 3.8. In 2022, 9 944 students enrolled in these programmes, marking a 9% increase from 2014. This sector is among the top five in demand. The popularity of BTS programmes in computing and data, despite the broader decline, underscores France's growing reliance on technology. Traditional fields may be losing appeal due to limited growth, while tech roles offer better job opportunities and adaptability, making them more attractive to students. Furthermore, national strategies and policy reforms, such as the inception of a national digital and computer sciences day, an expanded course offering, and improved information and career guidance on ICT sector, have amplified its allure (NSI, 2023[25]).

Figure 3.8. Enrolment in short-cycle tertiary level programmes and equivalent qualifications in service specialities by speciality, 2014 and 2022

Number of students by training specialisation



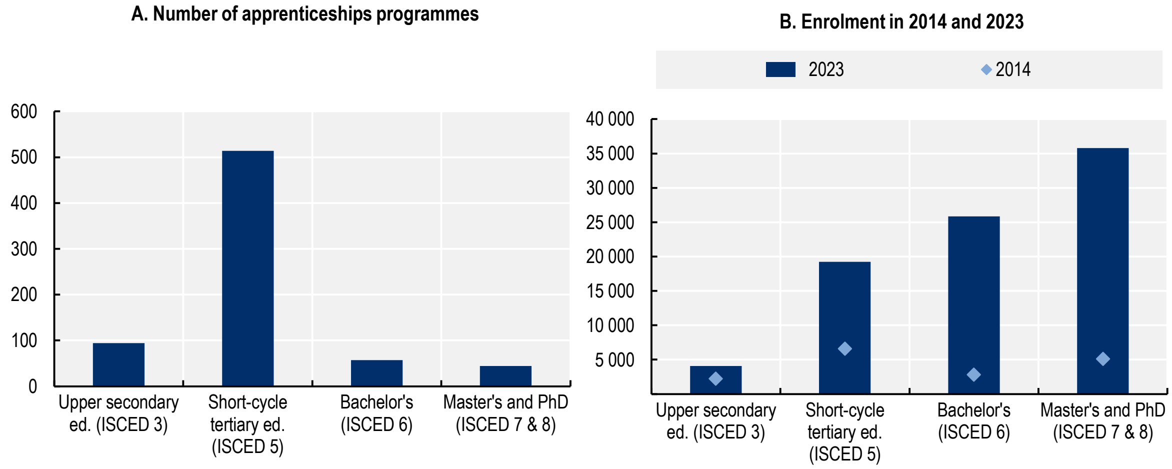
Note: Figures include all students enrolled in Higher technical sections (Sections de techniciens supérieurs, STS), upgrading classes for Advanced technician qualifications (Brevet de technician supérieur, BTS), National Diploma of Crafts and Design (Diplôme National des Métiers d'Art et du Design, DN MADE), bridging classes and Diploma in crafts and applied arts (Diplôme des Métiers d'Art, DMA) by training speciality in 2022-2023. 'Hairdressing, beauty care' includes other personal services specialism; 'Computing and information processing' includes data transmission professions; 'Image and sound techniques, related entertainment includes entertainment professions'; 'Cleaning, environmental protection' include sanitation related professions.
Source: DEPP (2023[9]), Repères et références statistiques, edition 2023, www.education.gouv.fr/reperes-et-references-statistiques-2023-378608.

Apprenticeships

Individuals can also opt for apprenticeships at initial levels to prepare for entry-level cyber security jobs. Apprenticeships combine classroom learning with real-world work, allowing apprentices to gain job-specific skills while working alongside experienced staff from the sector in addition to the more theoretical aspects of cyber security. Students can participate in apprenticeships at various levels – depending on their previous experience, their knowledge in the field, and -in some cases- their prior qualifications. There are apprenticeships targeting beginners in the field (equivalent to Vocational Baccalaureate or ISCED 3) to more experienced learners (equivalent to a master's degree or ISCED 7).

A significant imbalance exists despite the availability of cyber security apprenticeships at all levels: at short-cycle tertiary level apprenticeships positions are plentiful, but much higher enrolment in advanced-level apprenticeships (see Figure 3.9). As of October 2023, the ONISEP portal listed positions apprenticeship programmes, with the majority (72%) corresponding to short-cycle programmes (ISCED 5) (see Figure 3.9, Panel A). This indicates a commitment by educational institutions and employers to extend work-based learning to newcomers in cyber security. However, when it comes to actual enrolment, 72% of apprentices enrolled for bachelor's, master's, or doctoral level programmes (see Figure 3.9, Panel B). This trend towards advanced-level programmes is shaped by career aspirations and the enhanced employability associated with higher degrees. Moreover, employer preferences lean towards recruits with a deeper educational background for handling sophisticated tasks.

Figure 3.9. Number of cyber security apprenticeships positions and enrolment in ICT related apprenticeships in 2014 and 2023



Note: Upper secondary apprenticeships include Certificate of Vocational Aptitude (certificat d'Aptitude Professionnelle, CAP), Vocational Studies Certificate (Brevet d'Etudes Professionnelles, BEP), Professional certificate (Brevet Profesionnelle, BP), Vocational bacalaureatte (Bac professionnel); Short-cycle tertiary education includes Higher Technician section (Section de Techniciens Supériurs, STS); master's degree and PhD includes engineering programmes (Diplôme d'Ingenieur).
Source: MERS (2022[26]), Les effectifs d'étudiants dans le supérieur continuent leur progression en 2022-2023, www.enseignementsup-recherche.gouv.fr/fr/les-effectifs-d-etudiants-dans-le-superieur-continuent-leur-progression-en-2021-2022-88609; ONISEP (2023[4]), L'offre de formations de cybersécurité, www.onisep.fr/.

Enrolment in ICT-related apprenticeship programmes has increased significantly over the last decade, particularly at advanced levels, mirroring the sector's rapid growth and the escalating demand for specialised, high-level skills in the digital market, including cyber security. In 2023, close to 85 000 students were engaged in ICT apprenticeships, a fivefold increase from 2014 (see Figure 3.9, Panel B). The growth is even more pronounced at the higher educational levels (bachelor's and master's degrees), where enrolment has risen eightfold since 2014. This uptick is driven by government support for vocational education and the alignment of programmes with industry demands, ensuring apprentices are well-prepared for the evolving technological landscape. Additionally, tax incentives for companies employing apprentices and enhanced collaboration between higher education and the tech sector have been influential, multiplying opportunities and incentives for students (MTPEI, 2021[27]).

Bachelor's level

At the bachelor's level three types of qualifications may prepare for a career in cyber security: university bachelor's of technology (BUT), professional bachelor's and academic bachelor's degrees. The distinction between BUT programmes and professional bachelor's qualifications is rooted in their history. Until the 2021 reform, BUT programmes existed in a shorter form: two-year programmes led to a short-cycle tertiary qualification (*diplôme universitaire de technologie* or DUT). Graduates of DUT programmes commonly pursued an additional year of education, such obtaining a professional bachelor's qualification. Since the 2021 reform, the new BUT programmes are one year longer than their predecessor and lead to a bachelor's level qualification. Professional bachelor's programmes maintain their function of following up on short-cycle tertiary education, as they continue to offer a progression route to BTS graduates.

University bachelor's of technology programmes

University bachelor's of technology (BUT) programmes take three years to complete and are provided by University Institutes of Technology (IUT), nested within universities. BUT programmes target recent upper secondary graduates who seek to pursue higher education that prepares for careers in technology-related fields. Among 2021 entrants to BUT programmes, 57% held a General and 40% a Technological Baccalaureate. Only 1.5% of entrants held a Vocational Baccalaureate (ONISEP, 2023[28]). BUT programmes may be pursued either through the traditional route, with an internship (22-26 weeks over the three-year period of the programme), or through an apprenticeship route, alternating periods of school-based and work-based learning. The programme has an applied focus, and some courses are taught by professionals in the sector.

BUT programmes are available in the field of "Networks and telecommunications" (see Table 3.4). During the second year of studies, student must choose between four tracks, one being cyber security. The cyber security track allows students to acquire skills needed to administer and supervise secure information systems and respond to cyberattacks. Graduates are equipped with skills needed to implement security protocols and IT security compliance management within their relevant legislations (e.g. data protection) and government recommendations, which is one of the most relevant skills required for cyber security professionals in France (see Chapter 2). BUT programmes in networks and telecommunications may be accessed with a General or Technological Baccalaureate ("Sciences and technologies of Industry and sustainable development"). Access with a Vocational Baccalaureate ("Cyber security, ICT and networks") is possible if the candidate has a particularly strong profile. These programmes prepare for labour market entry, but a considerable share of graduates transition into an engineering school and graduate with an engineer qualification (at ISCED level 7).

Various progression routes are open to BUT graduates. After two years spent in a BUT programmes, students may transition to a bachelor's programme at a university. While BUT programmes are oriented towards labour market entry, graduates may also apply to a master's level programme upon completion. In addition, many engineering schools welcome students from IUT, through their parallel admissions. The number of places assigned to these profiles and the diploma specialties accepted vary from one school to another.

Table 3.4. Sample of University bachelor's of technology programmes

Institutions	Programmes	Description
IUT La Rochelle	BUT in computer sciences	The BUT Informatique aims to train IT professionals capable of participating in the design, creation and implementation of IT solutions serving users. Among the targeted areas: IT for business, embedded IT and connected objects, web applications, etc. To assume these responsibilities and adapt to the rapid evolution of ICT, computer scientists must be technologically competent, have good general knowledge and be adept at communication.
IUT Valence	BUT in computer sciences	The BUT is the perfect combination of educational and professional contributions. Part of the teaching is provided by professionals in the sector. This university degree is widely acclaimed by businesses.

Source: IUT La Rochelle (2023[29]) BUT informatique, www.iut-larochelle.fr/formations/departement-informatique/but-informatique/; IUT Valence (2023[30]), BUT informatique, www.iut-valence.fr/nos-formations/b-u-t-/b-u-t-info/b-u-t-informatique-776395.kjsp.

Professional bachelor's programmes

The professional bachelor's qualifications at bac+3 level, are provided mostly by IUTs, nested within universities. They allow students to acquire or deepen their theoretical and practical knowledge and skills in a particular sector or preparing for a specific profession. Prior to the 2019 reform, professional bachelor's qualifications were obtained through a one-year programme, which followed up on two-year DUT qualifications (MESR, 2022[31]). Since the reform, professional bachelor's programmes may be accessed directly after the completion of upper secondary education, or after one or two years of tertiary education (after gaining 60 or 120 ECTS credits). The duration of the professional bachelor's programme may now vary from one to three years, depending on the entry point of students.

Among the 173 specialisations on offer, several may focus on cyber security: "Computer Professions: Systems and Networks Administration and Security"; "Computer Networks and Telecommunications Professions"; and "Automated Systems, Networks, and Industrial Computing". The coursework includes theoretical and practical lessons, simulations of professional exercises, as well as a period of work-based learning in the company. One-third of the professional bachelor's programme includes individual and collective tutored projects or compulsory internships. A quarter of the lessons are taught by professionals in the field. Many professional bachelor's qualifications are pursued through an apprenticeship, alternating periods of school-based and work-based learning (see Table 3.5 for some examples).

Table 3.5. Sample of professional bachelor's degree

Institutions	Programmes	Description
École D'Ingénieurs (ECE)	Bachelor in cyber security	A bachelor's degree in cyber security is a bac+3 level diploma in digital data protection. It offers a common core of theoretical learning in order to understand areas related to IT security and to combine management and technology. This pogramme prepare students to learn and apply laws, systems, policies, and even concepts related to cyber security.
École D'Ingénieurs en Informatique (EPITA)	Bachelor in cyber security	This bachelor in cyber security allows students to acquire the fundamentals of digital technology while specialising in cyber security from the first year of the course. The programme includes numerous projects going beyond the simple application of lessons, allowing students to acquire technical, human and professional skills
École D'Ingénierus (ESAIP)	Bachelor of Computer Engineering and Cyber security	ESAIP offers a bachelor's in computer engineering in the areas of Cyber security and secure IoT & IIoT development. Learners take course on Virtualisation, Cyber security – Legal issues, SOC (Security Operations Center), and Encryption and VEP.

Source: ECE (2023[32]), Bachelor en cybersécurité, www.ece.fr/faq/bachelor-cybersecurite/; EPITA (2023[33]), Bachelor en cybersécurité www.epita.fr/bachelor-cybersecurite/ ; ESAIP (2023[34]), Bachelor en ingenierie informatique et cybersécurité, www.esaip.org/formation/bachelor-en-ingenierie-informatique-et-cybersecurite/.

Academic bachelor's programmes

Academic (non-professional) bachelor's programmes take three years to complete and are delivered within universities. Unlike professional bachelor's programmes, they are less oriented towards preparation for labour market entry. While students may pursue internships, those are not a mandatory part of the curriculum. Various bachelor's programmes prepare for employment in the digital sector and contain a substantial element of cyber security. Graduates of these bachelor's programmes are well-prepared mainly for further academic pursuits, including specialised master's degrees that offer deeper expertise in the field (see Table 3.6 for some examples).

Table 3.6. Sample of academic bachelor's programmes

Institutions	Programme	Description
École D'Ingénieurs (ESAIP)	Bachelor's in computer sciences	This programme has both theoretical and professional training, providing a mix of technical and soft skills required for middle managers for progressive careers. Students have the choice to specialise in one of the two areas of focus on during the final year: in cyber security and in web development.
École D'Ingénieurs (CESI)	Bachelor's in sciences and engineering	This programme prepares students to manage and optimise technology systems for enhanced business performance. It covers diagnosing system issues, managing maintenance projects, and implementing change. The curriculum emphasises project management, including agile and collaborative approaches, alongside the cultivation of essential soft skills for effective teamwork.

Source: ESAIP (2023[35]), Bachelor numerique, www.esaip.org/formation/bachelor-numerique/; CESI (2023[36]), Bachelor en sciences et en ingenierie, www.cesi.fr/programmes/cycle-bachelor-en-sciences-et-en-ingenierie/.

Academic bachelor's programmes have a broader focus (e.g. computer science) and do not specifically prepare for a career in cyber security. The curriculum of academic bachelor's programmes encompasses a broad spectrum of subjects, from the essentials of computer science to advanced topics in network security, ethical hacking, cryptography, and information systems security. Alongside technical skills, these programmes emphasise understanding the legal and ethical aspects of cyber security, critical for managing risks and protecting information in a professional setting. Although primarily taught in French, some programmes offer courses in English, thus attracting an international cohort.

The escalating frequency and sophistication of cyber threats have heightened the need for advanced cyber security programmes. In response to this demand, there's a marked increase in students advancing from bachelor's to master's programmes, with 38% of computer science higher education enrolment in 2022 dedicated to these advanced levels (see Figure 3.3). These programmes delve into specialised domains of cyber security, preparing students for the complexities of the field. Moreover, for those seeking to attain an even higher level of academic credential, prestigious grandes écoles offer engineering degrees, and doctoral studies provide avenues into research and teaching (see Box 3.3).

Non-formal training: The role of continuing education

Non-formal training in the field of cyber security is an increasingly popular alternative pathway to traditional academic routes, catering to the need for flexible and focused skill development. These trainings are offered by a diverse range of providers, including private training companies, industry associations, and online platforms. This type of training is characterised by its practical orientation, shorter duration, and often, the provision of certifications that are highly regarded by employers in the cyber security sector. Such non-formal programmes are designed to meet the demands of working professionals seeking to update their skills, career changers, and organisations looking to rapidly upskill their workforce in response to the dynamic cyber threat landscape.

In France, non-formal education programmes cover a wide range of courses, thus this section focuses in two of the most popular in the cyber security field: Continuing education programmes and certificate training.

Continuing education programmes (Formation continue)

Continuing education programmes (formation continue) are one of the multiple non-formal up- and reskill opportunities individuals have in several fields including cyber security. These programmes are tailored for professionals aiming to enhance their existing expertise or pivot their careers into the cyber security domain. Within continuing education programmes learners can engage with Institutional diplomas or certificates (Diplôme d'établissement) which are developed and conferred by educational institutions, offering them the flexibility to design programmes that swiftly respond to industry shifts and specialised professional requirements. These diplomas, while tailored to the institution's standards, are well-regarded within the professional sphere, especially when issued by reputable schools. An example of this diploma in the cyber security field is the "Certificat de Spécialisation en Cybersécurité" offered by multiples grandes écoles or universities. This training is collaboratively prepared with industry partners to ensure the programmes is in line with the latest cyber security trend and practices (see Table 3.9 for other examples).

Box 3.3. Diversity of advanced programmes in cyber security

Advanced programmes in higher education are crucial in the cybers security field due to the complex and ever-evolving nature of cyber threats. As cyberattacks become more sophisticated, there's a growing demand for professionals who are not only technically proficient but also equipped with strategic, management, and policy-making skills that advanced degrees tend to emphasise. Advanced programmes, such as master's and doctorates, often offer specialised tracks in areas like digital forensics, cyber law, risk management, and ethical hacking. They provide students with in-depth knowledge, research capabilities, and the critical thinking skills necessary to devise robust cyber security strategies and solutions.

These advanced programmes are available in various formats to accommodate different learning preferences and life circumstances.

Engineering programmes

Engineer qualifications are delivered in engineering schools at bac+5 level. The typical route into engineering programmes includes two years spent in highly selective preparatory courses. These courses (Classes préparatoires aux Grandes Écoles, CPGE) are two-year programmes that focus on a set of selected subjects (e.g. mathematics, physics and engineering sciences). They prepare students for entrance exams to the "grandes écoles", a selective and prestigious group of higher education institutions, which include engineering schools. Admission to some engineering schools is also possible upon completion of a short-cycle tertiary or a bachelor's qualification in a relevant field. Programmes lead to an engineering degree (a long first degree at ISCED level 7).

Table 3.7. Sample of engineering programme with cyber security component

Institutions	Programme	Description
Ecole Polytechnique de l'Université de Nantes	Computer engineering	The computer engineering course does not aim exclusively at this subject and does not include major courses linked to organisational security and defense issues. On the other hand, it provides numerous lessons essential to the progressive establishment of security skills from the bac+3 and bac+4 years: basic and advanced statistics, analysis and data mining, knowledge management, system of exploitation and databases, networks, cryptography, signal and image processing, then in the RSC option in the bac+5 year, a specific unit of systems and network security.
Telecom Paris Sud	Engineering	The "Systems and Network Security" is a specialisation of the general engineering track. During the last two years of the curriculum students are trained in cyber security, mameinly on fundamental technical aspects (network, protocols, system, virtualisation) but also on more emerging fields such as industrial systems or blockchains.
École Nationale Supérieure d'Ingénieurs de Bretagne Sud, ENSIBS	Cyber security engineering	The cyber defense specialisation trains professionals capable of understanding the threat and the modus operandi of attackers using a systems approach, and of building infrastructure security using a global approach, in order to better protect themselves and manage cyber crises.

Source: TELECOM SudParis (2023[37]), Sécurité des systèmes et des réseaux, www.telecom-sudparis.eu/formation/securite-des-systemes-et-des-reseaux/; INSA (2023[38]), Computer security and technologies (STI), www.insa-centrevaldeloire.fr/en/training/Information-technology-and-cyber security.

Specialised master's degrees

Specialised master's degrees in cyber security are designed to equip learners with advanced knowledge to protect digital infrastructures and respond to cyber threats. French institutions offer a variety of programmes that cater to different aspects of the field, from technical cyber defence to strategic and managerial cyber security studies. These programmes may focus on areas such as ethical hacking, digital forensics, information governance, and cyber risk management. Offered by leading universities and grande écoles, these courses often combine rigorous academic coursework with hands-on experience, including internships and partnerships with pioneering companies in the industry. Moreover, they frequently collaborate with national cyber security organisations, ensuring that the curriculum is aligned with current industry standards and the specific needs of the rapidly evolving digital security landscape.

Table 3.8. Sample of specialised masters in cyber security

Institutions	Programme	Description
Ecole Polytechnique	Executive MSc in Cyber security	The programme "Executive MSc in Cyber security" targets existing cyber security professionals who seek to deepen and update their technical expertise. The programme is designed to update basic competences in cyber security, consolidate existing skills and challenge participants in their approach to cyber security. The programme was introduced very recently, with first graduates of this programme expected to complete in early 2024. Participants typically pursue this programme with financial support from their employer and are released by their employer to be able to pursue their coursework (2.5 days per week).
Institut National des sciences appliquées Lyon, INSA	Specialised master's degree in digital cyber security	This training prepares auditors for four professional certifications highly appreciated by companies (Stormshield Network Security Administrator, iso27001 lead implementer, Ebios, Risk manager, CISSP). Each auditor is then free to take the official certification exam which will be billed directly by the certifying body. The cost of the certificate is not included in the price of the specialised master's degree. The MS was able to obtain a more advantageous rate for certain certifications.

Source: EP (2023[39]), Executive MSc in Cybersecurity, www.ip-paris.fr/en/education/lifelong-learning/executive-msc-cyber security; INSA Lyon (2023[40]), Cybersécurité du numérique, www.insa-lyon.fr/fr/mastere-cybersecurite-numerique

Table 3.9. Example of institutional diplomas or certificates in cyber security

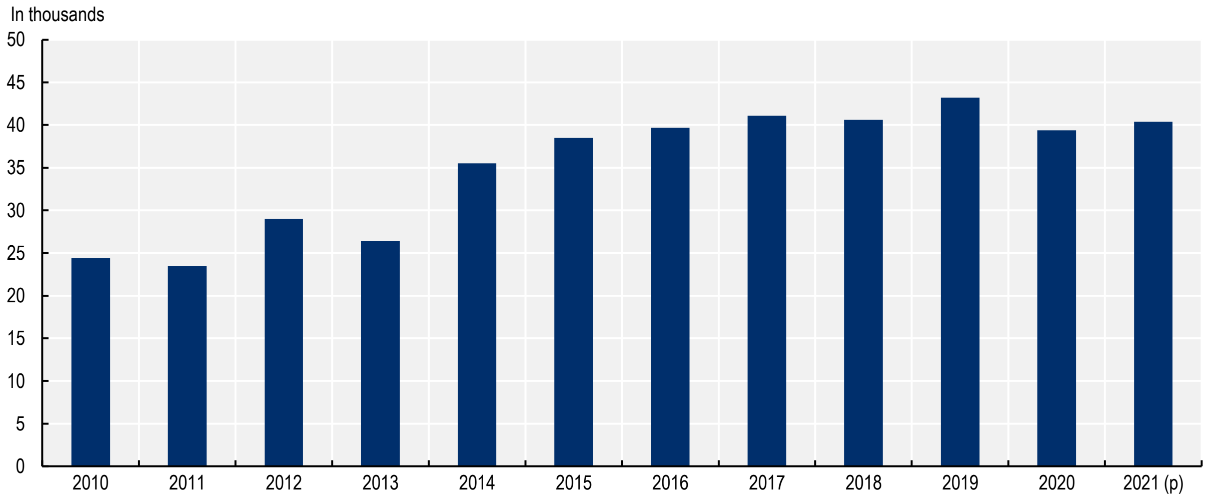
Institution	Programme	Description
TELECOM Sedaris	Certificate of specialised studies “information systems and network security”	This training provides trainees with the technical and organisational skills to define, deploy and manage a security architecture in the different professional contexts they will encounter. At the end of the training, participants will be able to: (1) Define the governance of the security of the company's information system; (2) Implement security mechanisms; (3) Develop and implement a security plan intended to the protection of the company's vital resources; (4) Design a security architecture. Participants who have successfully completed the tests and the professional project will be awarded the Specialized Studies Certificate “Information systems and network security” issued by Telecom SudParis.
CNAM Paris	Cyber security Analyst Skills Certificate	This training targets professionals with at least a two-year degree in computer science or a scientific/technical field, plus IT experience. Prerequisites include foundational units in networking, with recommendations to complete basic cyber security courses. This certification equips individuals with the ability to manage and secure network infrastructures, participate in IT architecture development, and support IT systems with an emphasis on security. It encompasses technical skills for equipment management, performance monitoring, and technical support, alongside strategic competencies for risk management, policy formulation, and incident response in corporate cyber security environments.

Source: CNAM Paris (2023[41]), Certificat de compétence Analyste en cybersécurité, www.cnam-paris.fr/certificat-de-competence-analyste-en-cybersecurite-1263707.kjsp; TELECOM SudParis (2023[42]), Certification professionnelle à la Gouvernance de la sécurité des systèmes d'information et des réseaux, www.telecom-sudparis.eu/formation/ces-securite-des-systemes-information-et-reseaux/.

Entrance into a “Diplôme d'établissement” cyber security programme usually requires a background in computer science or a related discipline, with additional prerequisites that may include certain IT competencies or preliminary courses. After completing this targeted diploma, graduates are poised for immediate entry into the cyber security job market, leveraging their specialised training to meet industry demands. For those looking to deepen their expertise, further educational pursuits or professional certifications are viable next steps, opening doors to advanced security roles or managerial positions within the cyber security sector.

Regardless of the field, the number of continuing education courses offered, and the diplomas awarded have been increasing, indicating a growing demand for short, concise courses focused on imparting specific, highly sought-after skills in the job market (DEPP, 2023[9]). In 2021, around 40 400 institutional diplomas were awarded, nearly double the number offered in 2010 (just over 24 000) (see Figure 3.10). A similar pattern is found for courses in the field of computer science, including cyber security. In 2022, around 9 250 people have been trained, including through continuing education programmes, to become specialists in the field at all levels (MFIDS, 2022[43]), thanks to the national acceleration strategy for cyber security, developed by the French Government (MFIDS, 2021[44]).

Figure 3.10. Diplomas awarded on completion of continuing education



Note: Figures includes all diplomas awarded in all fields and specialisations including those related to computer science. Value for 2021 is projected (p).
Source: DEPP (2023[9]), Repères et références statistiques, edition 2023, www.education.gouv.fr/reperes-et-references-statistiques-2023-378608.

Certifying or certificate training offered by specialised providers (Formation certifiante)

These are certification-oriented educational programme that offer a mix of theorical and practical training that culminates in credentials recognised in the industry. In contrast to the “Diplôme d'établissement” programmes, these certificates are provided mostly by specialised providers or relevant companies in the cyber security field. With their emphasis on direct applicability and the fast acquisition of in-demand skills, these programmes are ideal for professionals aiming to quickly enhance their expertise or break into the cyber security field.

A wide range of certificate training programmes are available in the field of cyber security. This study focuses on three of them. A “simple certificate (attestation simple)” refers to a basic form of certification or acknowledgment for completing a training course. It does not involve any rigorous examination process or compliance with international standards. The ANSSI, through the SECNUMEDU-FC certification, recognises certifying non-formal training that meets its quality standards. In 2023, there are 60 simple certificate training programmes recognised by ANSSI, covering multiple specific competencies and at different levels of difficulty (ANSSI, 2023[45]). (Table 3.10 shows some examples.)

Table 3.10. A sample of certificate training recognised by ANSSI through SECNUMEDU-FC certification process

Type of certificate	Providers	Programme	Description
Simple certificate	MIRAT DI NERIDE	Risk analysis: use of the EBIOS method, a new challenge for decision-makers	This cyber security training, targeting business leaders and managers, focuses on risk analysis via the EBIOS method through five practical workshops. Led by a consultant with extensive experience and an MBA from the Sorbonne, it requires no prior tech knowledge and uses real case studies and direct interaction to equip leaders with the skills to assess and manage risks, ultimately enhancing business value.
	STORMSHIELD	Certified stormshield network administrator (csna)	The CSNA training combines theoretical lessons and practical work to enable the trainee to set up an SNS firewall in a computer network. This will allow it to ensure the security and integrity of its architecture against internal and external attacks. The implementation of this security will be reinforced by learning different methods of authenticating computer system users as well as by setting up virtual private networks (VPN).

Type of certificate	Providers	Programme	Description
	FITEC	Cyber security consultant	This training allows trainees to be operational, from the end of the training, on all the modules and actions followed during it. They can thus be recruited and integrate projects as junior consultants with solid foundations to progress very quickly in the world of cyber security. This allows them to stay in the area targeted by the training and address different cyber security topics.
ISO/IEC 17024 training certificates	EduGroupe	Certification risk manager ISO27005	The “ISO/IEC 27005 Risk Manager” training will allow learners to develop the skills necessary to master the risk management processes linked to all assets relevant to information security using the ISO/IEC 27005 standard as a reference framework.
	H2S	ISO 27001 lead auditor	With this training students learn to audit according to the ISO27001 standard and associated guides, to have the auditor's vision with regard to the ISO 27001 standard, to integrate the PDCA model during audit activities, to audit the different categories of measures security (Annex A of ISO27001 / ISO27002) and conduct an ISMS audit and its interviews by mastering the concepts of major or minor non-conformities.
	FIDENS	Certification – ISO 27001 fundamentals	The certification ensures that the holder masters best practices in auditing, managing, monitoring, remediating and improving information security management systems, in order to secure sensitive information and improve the overall performance of the organisation in information security. In terms of know-how, this certification meets the needs of the national and international market, all sectors of activity.

Source: ANSSI (2023[45]), Formations continues labellisées secnumedu-FC, www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu/.

Learners can also engage with ISO/IEC 17024 certified training programmes, which are aligned with an internationally recognised standard. This ensures that professionals holding certifications in cyber security have been evaluated rigorously and fairly, based on global benchmarks for their skills, knowledge, and abilities. Adherence to ISO/IEC 17024 guarantees a certification process that is transparent, impartial, and of consistent quality, fostering trust and recognition in the expertise of certified cyber security professionals worldwide. As of 2023, ANSSI has recognised 20 ISO/IEC 17024 training programmes and is planning to expand this offering in 2024 (ANSSI, 2023[45]).

Box 3.4. Online courses in digital skills available in French: Insights from e-learning platforms

In France, the top e-learning platforms like Udemy, CodeAcademy, Coursera, and LinkedIn Learning (Leptidigital, 2023[46]) offer around 10 100 online courses. Approximately 21% focus on digital subjects (see Table 3.11). Although the availability of cyber security courses is limited, LinkedIn Learning and Udemy stand out with the most extensive selections, providing 917 and 881 French-language courses respectively, as of July 2023. These platforms cater to learners of all levels ranging from beginners to those pursuing advanced certification programmes and budgets. Some of these courses may be free for learners. Beginners can enroll in courses such as ‘Computer security and digital dangers (Sécurité informatique et dangers du numérique)’, while more experienced learners can explore options like ‘Cyber security: How to secure a website (Cybersécurité: comment sécuriser un site web)’. Some courses are aligned with competency certifications or industry standards. For example, Udemy provides training for cyber security certification such as ‘(ISC)2 certified in cyber security’, which holds high relevance in the sector.

Table 3.11. Online short courses offered in French on a selected of e-learning platforms

Online training provider / Platform	Total number of training courses (approx.) *	Total number of courses offered in digital skills and computer sciences	% Out of the total number of courses offered	Total number of courses offered in cyber security	% Out of the total number of courses offered in computer sciences
Udemy	6 000 +	881	15	132	15
Coursera	500 +	285	57	13	5
LinkedIn Learning	3 200 +	917	29	74	8
CodeAcademy	400+	19	5	16	84
Total	10 100+	2102	21	235	11

Note: The numbers for digital and computer science and cyber security were retrieved from each platform course finder. The filters available by default were used for the number of digital and computer science courses. For the number of cyber security courses, "cyber security" word combinations were used in each platform's search engine after filtering by digital and computer science fields. Only the courses offered in French were taken into account. The total number of training courses is taken from the e-learning platform websites(*).
Source: Information collected on line directly from providers' platforms in July, 2023.

The Professional Qualification Certificat (Certificat de Qualification Professionnelle, CQP) is an industry-recognised French certification denoting an individual's capability to perform a specific role, particularly within technical or vocational domains (MTPEI, 2017[47]). Acting as a skills and competency benchmark, these certificates are driven by sector-specific professional organisations to meet workplace standards. Within cyber security, CQPs hold significant value due to the field's specialised requirements. They affirm a professional's proficiency in roles ranging from security analyst to incident responder, aligning with the pressing demand for experts adept at countering cyber threats and safeguarding information. Cyber security CQPs prioritise practical, job-related skills and knowledge required to meet the exacting expectations of employers in this crucial sector.

Finally, numerous online platforms provide French-language cyber security courses, broadening the accessibility of specialised training (see Box 3.1). These courses serve a spectrum of learners, offering flexible, self-paced learning environments from foundational to advanced levels. The flexible way of provision and interactive nature of online courses, coupled with certification options, make them an attractive avenue for those seeking to enter or progress in the cyber security field.

A framework for the development of cyber security education

The place of cyber security in key national strategies

The background to current efforts to enhance cyber security education is the National Strategy for Cyber Security, supported by a EUR 1 billion investment package (Box 3.5). This infusion of resources is dedicated to elevating the nation's cyber defences through advanced education, innovative research, and specialised training programmes, aimed at cultivating a skilled cyber security workforce.

Box 3.5. Educational focus and workforce development in France's cyber security strategy

The French National Acceleration Strategy for Cyber Security outlines the country's approach to strengthening its cyber defences and ensuring the digital security of the state, its citizens, and its businesses by fostering research and development, and educating and training skilled workforce.

The strategy is supported by a EUR 1 billion investment package, part of France Relance and the Future Investment programme, which was announced in 2021. Its key targets for 2025 are:

- Triple turnover in the sector (from EUR 7.3 billion to EUR 25 billion).
- Position France in relation to international competitors by doubling the number of jobs in the sector (from 37 000 to 75 000).
- Restructure the sector and reposition France in relation to international competitors in terms of the number of companies in the sector.
- Support the emergence of three French cyber security unicorns (i.e. highly valued, privately held startups specialising in innovative cyber security solutions), leveraging major startups in the industry, especially those within the French Tech 120.
- Promote a cyber security culture within companies.
- Stimulate French research in cyber security and industrial innovation, aiming for a 20% increase in patents.

France's national cyber security strategy places a strong emphasis on education and raising awareness to create a skilled cyber security workforce (MFIDS, 2022[43]). The strategy involves integrating cyber security into educational curricula across all levels (from basic to higher education), fostering a culture of digital hygiene from a young age, and developing specialised university programmes to cultivate a skilled cyber security workforce. It also encompasses ongoing professional development through targeted training and certification programmes. Public awareness campaigns, delivered via ANSSI and reinforced through public-private partnerships, further educate citizens on safe online practices and data protection. This comprehensive educational approach is pivotal to France's vision of strengthening its national cyber security posture by ensuring that every individual is informed and vigilant in the digital space.

Source: Gouvernement (2021[48]), Un plan à 1 milliard d'euros pour renforcer la cybersécurité, www.gouvernement.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite.

A major challenge is to anticipate future skills needs, identifying professions and competences of the future, as well as those that will be less needed (including within the field of cyber security, as for example artificial intelligence reshapes how cyber security professionals work).

The programme “Competences and professions of the future 2021-2025” (“AMI-CMA” in French) is a key tool to help the education and training system respond in an agile way to expected skills needs. AMI-CMA is part of the broader strategy “France 2030”. The first wave was launched in 2021 and ended in March 2023. The second wave started in May 2023. In the context of efforts to support re-industrialisation and sovereignty, major skills gaps appear in various fields: in particular the digital economy, healthcare and food. The AMI-CMA programme aims to train 400 000 people per year by 2030 and yield one million new graduates by 2030 at various levels: operators, technicians, engineering assistants, engineers, as well as master's and doctoral graduates, mostly in STEM fields. The AMI-CMA programme contains two elements. The first is diagnostic: assessing skills needs in the light of existing education and training programmes, in order to identify priorities for investment. The second element is training: developing new education and training programmes. New programmes must build on a prior diagnostic that identified a gap. They are then developed through a consortium that includes employer representatives and a training provider (e.g. university, school, apprentice training centre) (ANR, 2021[49]).

The Ministry of Higher Education and Research emphasises the importance of three levels of expertise and related education programmes in cyber security. First, it seeks to develop good digital hygiene habits in the entire population, so that cyber security becomes a "reflex". Efforts in this area target in particular higher education students, but also include initiatives at lower levels of education. Second, efforts aim to ensure that individuals are equipped with skills needed to use existing cyber security solutions. This targets higher education students, mostly at short-cycle tertiary and bachelor's level. The third area of interest is to develop a talent pool of individuals who can develop cyber security solutions. This involves advanced higher education programmes, including engineering programmes, master's and doctoral programmes. Efforts focus also on supporting research, both in private and public entities.

Box 3.6. Cyber security in management: Global tech & cyber security pathway, Rennes School of Business

This innovative hybrid programme was introduced in 2021, based on the idea that all managers need a solid understanding of issues linked to new technologies, in particular artificial intelligence and cyber security. The programme leads to a bac+5 qualification and entrants have typically completed a two-year preparatory course (or a first tertiary qualification at short-cycle tertiary or bachelor's level). The programme includes modules such as the "Geo-economics of tech" or "Artificial intelligence and strategy". Students may opt for this pathway already in their first year of studies, or may change later. About a third of the coursework focuses on global tech and cyber security (within that 70% focuses on cyber security). During the second year of studies students specialise in their preferred area through a package of optional courses (e.g. Analysis of cyber threats, Entrepreneurship in cyber security, Programming). This programme aims to recruit as many females as males.

In addition, a new double-degree programme is currently under development. It will include Rennes School of Business and the engineering school IMT Atlantique Bretagne-Pays de la Loire. The content will combine management (about 70% of course content) and technical skills (about 30%) relevant for cyber security.

Source: Rennes SB (2021[50]), Rennes School of Business ouvre son nouveau parcours « Global Tech & Cyber security », www.rennes-sb.fr/programmes-fr/nouveau-parcours-global-tech-cyber security-programme-grande-ecole/.

Within higher education, one question is at which level cyber security programmes are, or should be, offered. Interviews conducted with policy makers in higher education suggest that the overall vision is that during the first years of higher education students tend to develop a broader set of skills within their field of study. Higher levels of specialisation usually happen at later stages, mostly five years into higher education – in the form of long first-degree programmes, such as those offered by engineering schools, or master's degrees. The balance between bachelor's level profiles and master's level profiles (including engineers) is about a quarter for the former and three quarters for the latter. Companies seeking to recruit an information systems security manager typically require an engineering degree. This reflects the broader role of engineering schools in supplying advanced technical skills within the French economy. Finally, PhD graduates play a key role in supporting innovation efforts in the field of cyber security, both within the public and the private sector.

In addition, there is recognition among policy makers and higher education providers that it is necessary to include an element of cyber security in some programmes outside the digital sector. Examples include law and marketing – programmes that train future professionals who have an important role to play in the case of cyberattacks or in providing cyber security solutions. Box 3.6 provides an example of how cyber security is integrated into a management programme.

Box 3.7. Creating a common skill framework for the cyber security profession in Europe

European Cyber security Skill Framework (ECFS)

The European Cyber security Skills Framework (ECSF) is a practical tool to support the identification and articulation of tasks, competences, skills and knowledge associated with the roles of European cyber security professionals. It is the EU reference point for defining and assessing relevant skills, as defined in the Cyber security Skills Academy, which was recently announced by the European Commission.

The ECSF summarises the cyber security-related roles into 12 profiles, which are individually analysed into the details of their corresponding responsibilities, skills, synergies and interdependencies. It provides a common understanding of the relevant roles, competencies, skills and knowledge mostly required in cyber security, facilitates recognition of cyber security skills, and supports the design of cyber security-related training programmes.

The Cyber Security Skills Academy

Within this context, in April 2023, the Commission adopted the Communication on a Cyber security Skills Academy, a policy initiative which aims to bring together existing initiatives on cyber skills and improve their co-ordination, with a view to bridging the cyber security talent gap and boosting competitiveness, growth and resilience in the EU. The ECSF constitutes the basis on which the Academy will define and assess relevant skills, monitor the evolution of the skill gaps and provide indications on the new needs.

Source:ENISA (2022[51]), European Cybersecurity Skills Framework (ECSF), www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework.

The French Cyber security strategy is closely intertwined with broader European efforts, such as Horizon Europe and the Digital Europe Programme, to establish a cohesive cyber security skillset across the EU. Anchored by the European Cyber security Skills Framework, these collaborative measures aim to harmonise skills qualifications and ensure a standardised approach to cyber defence (see Box 3.7). Additionally, the Cyber security Skills Academy in the European Union serves as a hub for professional training, further amplifying the strategy's effectiveness (see Box 3.7). France’s active involvement in these initiatives fosters a harmonious integration of expertise and resources, reinforcing a shared infrastructure of cyber security capabilities that safeguard the interconnected network of the EU. These concerted actions are pivotal in bolstering the region’s digital resilience against an array of cyber threats.

Giving visibility to cyber security in education programmes

Two quality labels have been developed to signal high-quality cyber security content in education and training programmes. The two labels are designed for two different levels of expertise, reflecting the idea that ensuring cyber security requires not only skilled professionals with technical cyber security skills, but also some knowledge of cyber security issues among those working in a broader set of professions. The first label focuses on programmes that include an element of cyber security within professions linked to the digital sector. The second label focuses on highly technical programmes, that develop specialised technical skills in cyber security, preparing professionals for entry into employment as a cyber security specialist. Both labels are discussed in detail below.

Foundational cyber security skills for digital sector professionals

Several higher education institutions that prepare for employment in the digital sector seek to go beyond raising awareness. They integrate a stronger element of cyber security in their programmes, but do not train specialised cyber security professionals.

ANSSI established the label CyberEdu to signal education programmes within the digital sector that integrate an element of cyber security. Its development followed the publication of a White Paper on Defense and National security in 2013. The CyberEdu label is designed to help the introduction of cyber security concepts into all digital-related training programmes in France. The goal is to ensure that all those involved in the information systems chain (e.g. administrators, developers, project managers) feel concerned, as digital security also requires the engagement of those who are not experts in the field. The approach seeks to improve vigilance and incident response, limit vulnerabilities in information systems, and facilitate co-operation with cyber security specialists. All professionals need to be aware, initiated, or even trained in cyber security without necessarily becoming experts in the field.

The Association CyberEdu was established to help implement efforts in this area. It brings together computer science teachers, cyber security specialists, and non-specialists, to promote the CyberEdu approach throughout the country. Their activities include developing pedagogical tools, organising events and communication regarding cyber security, and certifying training programmes. These efforts are aligned with the National Strategy for Cyber security, presented by the prime minister in 2015. This strategy outlined two objectives that are related to CyberEdu: integrating cyber security awareness into all higher education and continuing education programmes; and integrating cyber security training into all higher education programmes that include a component of computer science (CyberEdu, 2022[52]).

One of the Vocational Baccalaureate programmes is certified by CyberEdu: “Cyber security, ICT and networks”. In addition, several short-cycle tertiary qualifications are certified by CyberEdu. The main programme at short-cycle tertiary level is the “BTS in information technology services for organisations”. It has two options: “Infrastructure, systems and networks solutions” and “Software solutions and business applications”. Both options contain cyber security as one of the three key competence areas targeted by the programme. These programmes may be accessed with different types of baccalaureat: the Vocational Baccalaureate in “Cyber security, ICT and networks”, or a Technological Baccalaureate (either “Sciences and technologies of management and administration” or “Sciences and technologies of Industry and sustainable development”). Admission is also possible with a general baccalauréat. While most graduates will enter the labour market upon completion, it is possible to progress to a professional bachelor’s programme in the same field. Finally, several bachelor’s programmes have gained the CyberEdu quality label. This includes both bachelor’s programmes, as well as professional bachelor’s programmes (Table 3.12 provides some examples).

Table 3.12. Examples of programmes with CyberEdu Certification

Institution	Programme	Description
Paris-Est Créteil	Bachelor's in Economics and Management - Computer Science and Management Track	This dual-focused approach equips students with competencies in IT development and business management. The programme is distinguished by two key elements: fostering creativity and instilling cyber security awareness. These aspects are further enriched by the option for students to simultaneously enroll in the University Diploma for Innovation and Cyber security.
University of Toulon	Bachelor's in Computer Science - Computer Science Track	The three-year IT course offers an integrated education in IT and applied mathematics, enriched by practical modules and English proficiency. It prepares students for advanced studies or direct entry into the tech industry, serving as a gateway to the Toulon region's tech enterprises such as DCNS and Bull SAS.

Institution	Programme	Description
IUT Haguenau	Professional Bachelor's in Automated Systems, Networks, and Industrial Computing, Industry of the Future Option	The Professional License programme melds 450 hours of classwork with 150 hours of project supervision and includes a 12 to 16-week professional placement. Tailored for those with a bac+2 qualification, the curriculum—shaped by industry experts—ensures graduates' employability and career progression. Offered as a concise two-semester programme, it confers 60 ECTS credits and caps at 180 credits, with limited enrollment to ensure personalised supervision.
IUT de Ville d'Avray	Professional Bachelor's in Industrial Production Management, Industrial Computing, Automation, and Production Option	The professional license programme crafts experts in industrial computing and automation, pivotal for future-oriented industries and smart systems. The hands-on curriculum prioritises practical skills, delivered in small, focused groups on a state-of-the-art Industry 4.0 platform, ensuring graduates are in high demand, as reflected by the significant apprenticeship uptake, reaching 100%.

Source: UPEC (2023[53]), Licence economie et gestion parcours informatique et management, www.u-pec.fr/fr/formation/niveau-l/licence-economie-et-gestion-parcours-informatique-et-management-miage; Université de Toulon (2023[54]), Licence informatique parcours informatique www.univ-tln.fr/Licence-Informatique-parcours-Informatique.html; IUT Haguenau (2023[55]), Systemes automatises, reseaux et informatique industrielle, https://iuthaguenau.unistra.fr/formations/licence-pro/systemes-automatises-reseaux-et-informatique-industrielle; IUT Ville d'Avray Saint-Cloud Nanterre (2023[56]), Licence professionnelle i2ap, https://cva-geii.parisnanterre.fr/formations/licence-professionnelle-i2ap.

Advanced technical skills for future cyber security professionals

The Digital Security Education (Sécurité Numérique éducation or SecNumedu) label was developed to identify high-quality specialised programmes in cyber security. This accreditation is awarded by the ANSSI, the French National Agency for the Security of Information Systems, which serves as the country's chief authority on defending its information systems. The SecNumedu label recognises courses that meet a high standard of quality and provide relevant, comprehensive training in the field of cyber security. It covers a wide range of programmes, from entry-level cyber security courses to more advanced and specialised courses, each catering to different aspects of cyber security such as network security, data protection, cyber threat intelligence, and ethical hacking.

The benefits of the SecNumedu label are substantial for both educational institutions and learners. For institutions, having the SecNumedu label denotes a recognised quality standard for their programmes, which can help attract more learners, foster institutional prestige, and, in turn, support the continuous development of the cyber security field. For learners, enrolling in a SecNumedu labelled programme ensures that they receive up-to-date, comprehensive, and high-quality education in cyber security. Additionally, a certificate from a SecNumedu accredited course can enhance their employment prospects, as employers often look for candidates with recognised qualifications in the competitive field of cyber security. By ensuring a certain standard of training, the certification benefits the entire ecosystem - it helps the institutions to maintain quality education, and it helps the learners to gain relevant and recognised skills in the cyber security domain.

The SecNumEdu label concerns mostly engineering programmes and master's programmes, but it is also associated with some professional bachelor's degrees. Table 3.13 provides some examples of programmes that have obtained this label.

Table 3.13. Examples of programmes with SecNumEdu label

Institution	Programme	Description
IUT of Blois, François Rabelais University of Tours	Professional license in quality – information systems security (QSSI)	The QSSI equips students with the skills to maintain information system integrity and security in professional settings. The programme blends technical training in security tools and quality management with essential IT and soft skills, culminating in practical projects and on-the-job training through internships or apprenticeships.
EFREI Paris	Engineer graduated, major in cyber security, information systems and governance (CSIG)	The CSIG Major in the engineering cycle's final two years trains Cyber Engineers in functional security and offers paths to attain ISO 27005 and ISO 27001 certifications. Alongside technical expertise, the programme emphasises "soft skills," preparing students for the multifaceted challenges of cyber security.

Institution	Programme	Description
University of Poitiers - Niort Campus	Master in risks and environment, information systems risk management (MRSI) course	This programme crafts leaders in risk management, specialising in Information Systems Risks (RSI) that underscore IS security, bolstered by IRIAF's FRUIT cyber range. The curriculum, blending multidisciplinary research with practical internships, progresses from engineering to strategic management skills, preparing graduates for high-demand roles in IS security management, consulting, and risk auditing.
INSA LYON (National Institute of Applied Sciences of LYON)	Specialised master in digital cyber security	This programme offers a comprehensive 500-hour curriculum in cyber security governance and engineering, with an array of industry-recognised certifications. Lauded as the second-best programme of its kind in France, it boasts a faculty predominantly comprised of industry experts. Participants enjoy the convenience of on-campus accommodations and dining facilities.

Source: ANSSI (2023[57]), Se former à la cybersécurité, https://cyber.gouv.fr/se-former-la-cybersecurite.

Industry involvement in the delivery of programmes

This section focuses on two kinds of industry involvement in the delivery of education programmes in the field of cyber security. The first part describes the use of work-based learning in cyber security programmes. The second part explores the involvement of professionals in cyber security in teaching future professionals in the field.

Providing work-based learning opportunities in the cyber security sector

An element of work-based learning is commonly used in programmes that focus on cyber security (as well as other professionally-oriented programmes). Work-based learning, especially through apprenticeships, offers graduates an edge by fostering close ties with specific companies and industries, often leading to more permanent job placements right from the start (Couppié and Gasquet, 2021[58]). Thus, the inclusion of a mandatory internship is a quality criterion for obtaining a SecNumEdu label. For example, three-year programmes leading to a Vocational Baccalaureate require 18 to 22 weeks to be spent in work-based learning (ONISEP, 2023[59]). BTS, DUT, professional bachelor's and engineering programmes either involve a mandatory internship or may be pursued through an apprenticeship, alternating periods of work-based learning with classroom learning (see Table 3.8). For example, at the Saint Malo University Institute of Technology apprenticeship is a common route to BUT qualifications. Among first year students 30% pursue an apprenticeship, among second year students 60% do so, while all third year students pursue this route. This typically involves alternating one month spent within the IUT and one month spent with an employer.

Table 3.14. Types of work-based learning in education programmes

	Mandatory work-based learning	Duration	Type of work-based learning	Example of work-based learning opportunities in the cyber security field
Vocational baccalaureat	Yes	18-22 weeks	Internship (*Stage*) Apprenticeships (*Apprentissage*)	• Cyber security assistant • IT technician on work-study scheme
BTS	Yes	4-8 weeks spread over the two-year programme.	Internships	
BUT	Yes	12-16 weeks for internships 18-22 weeks for apprenticeships	Internship Apprenticeships	• IT Operations Technician • Systems and networks technician
Professional bachelor's	Yes	12-16 weeks	Internship Apprenticeships	• Systems and networks administrator • IT systems and software consultancy
Bachelor's	No	4-16 weeks	Internship (Optional)	

	Mandatory work-based learning	Duration	Type of work-based learning	Example of work-based learning opportunities in the cyber security field
Engineering	Yes	4-6 weeks for first-year discovery internship 12-22 weeks for mid-curriculum internship	Internship Apprenticeships	• Cyber security and IoE engineering's Apprenticeship • Manager in IT infrastructure and cyber security on a work-study basis
Master's or PhD	No	16-24 weeks for internships 24-48 weeks for apprenticeships	Professional Internship or Research Internship (Optional) Apprenticeship (Optional)	• Work-based master's degree in cyber security

Note : BTS refers to Brevet de Technicien Supérieur and BUT refers to Bachelor Universitaire de Technologie.
Source: ONISEP (2022[60]), Les stages dans l'enseignement supérieur, www.onisep.fr/vers-l-emploi/stages-en-entreprises/les-stages-par-niveau-d-etudes/les-stages-dans-l-enseignement-superieur; ONISEP (2023[59]), Les stages en Lycée professionnel, www.onisep.fr/vers-l-emploi/stages-en-entreprises/les-stages-par-niveau-d-etudes/les-stages-en-lycee-professionnel.

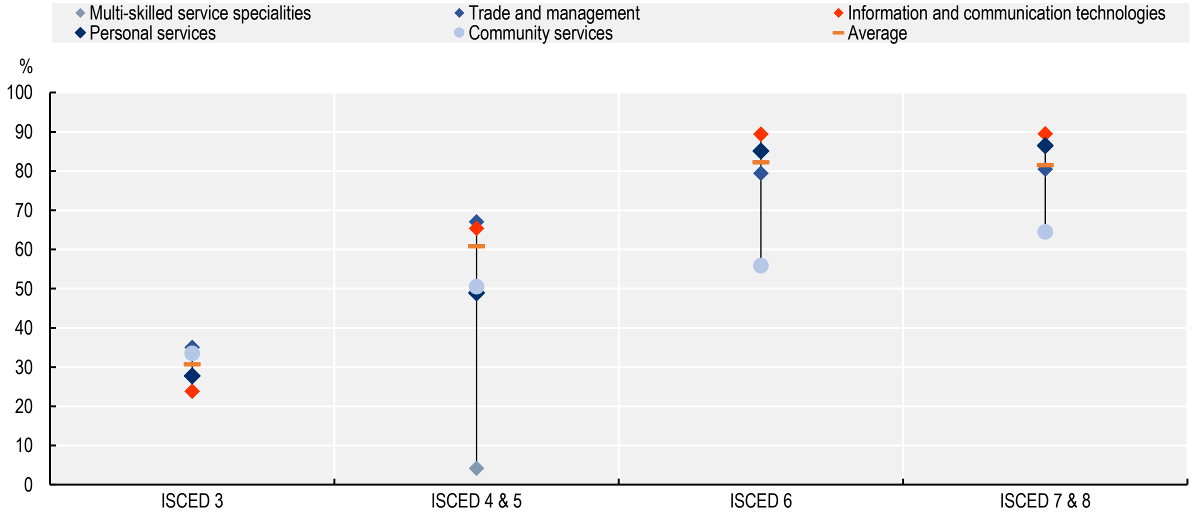
Participation in apprenticeships has increased significantly over the last decade, particularly in the ICT field (see Figure 3.11). The number of ICT apprentices has risen by 80% since 2014, which is nearly 20 percentage points higher than the average for all fields within the service sector. While apprenticeship enrollment has climbed at all levels and across all fields, it has been predominantly concentrated at higher educational levels, including bachelor's, master's, and Ph.D. programmes. Specifically, the number of ICT apprentices at these advanced levels has almost doubled in 2022 compared to 2014. As technology rapidly advances, there is a pressing need for a highly skilled workforce with expertise in areas such as cyber security, data science, and software development. Higher education institutions have responded by creating more apprenticeship opportunities that dovetail with advanced degree programmes, offering students the dual advantage of academic credentials and practical, work-based experience. Moreover, businesses are increasingly recognising the value of integrating apprentices into their workforce, not just for the fresh perspectives and current academic knowledge they bring, but also as a means of developing a talent pipeline tailored to their specific technological and operational needs.

Some institutions, in particular engineering schools, report that those pursuing an apprenticeship route have a different profile compared to those who pursue their education in classroom settings with an internship. Graduates of BTS or DUT programmes already have some experience of workplaces, and in some programmes tend to pursue apprenticeships, while those admitted through preparatory courses more often pursue a school-based route with an internship. Another potential reason for this is that admission results after preparatory courses (and subsequent tests) are announced during the summer, while the recruitment for apprentice engineer positions tends to happen over the spring or early in the summer.

Upper-secondary and higher education institutions use different strategies for establishing connections with companies that provide internships or host apprentices. Many have built a network of partner companies, through prior professional connections, alumni networks as well as links to the local economy. Internal platforms allow students to connect with opportunities offered by employers, or students may find suitable opportunities on their own. In the field of cyber security, there is a diverse range of potential employers that offer work-based learning opportunities. Options include start-ups, in the digital sector or elsewhere, large private-sector companies as well as the public sector (e.g. ministries). Providers tend to report that it is easy to find placements for students, as the sector faces skills shortages and employers are keen to train and identify potential future recruits. There is also some variation across providers in how different schedules for those pursing an apprenticeship vs. those in school-based settings are organised. Some providers report high degrees of personalisation in terms of schedules, with the use of hybrid forms of teaching (online and in-person). Others schedule in-person lessons in a way that it is compatible with the schedules of both school-based students and apprentices.

Figure 3.11. Apprenticeships enrolment growth between 2014 and 2022, by field of study in the domain of services

In percentage change



Note: In educational contexts, "Services" as a field of study broadly covers service-oriented sectors such as hospitality, tourism, health and social care, business, and information and communication technologies services. This term typically includes vocational and professional training programmes in these non-industrial, non-agricultural areas, especially relevant in discussions of apprenticeship enrolment growth.
Source: DEPP (2016[61]), Repères and references statisques, www.education.gouv.fr/sites/default/files/imported_files/document/depp_rers_2016_614975.pdf.

Bringing cyber security professionals into the teaching workforce

At upper secondary level it is uncommon for teachers of vocational subjects to pursue parallel employment in the private sector. However, regulations allow for and encourage experienced professionals to move into the teaching profession. Teaching as a contractual or substitute teacher is possible without taking the national examination. Such non-tenured teachers allow to respond in a flexible way to changes in demand and tackle challenges related to tenured teacher shortages. Becoming a non-contractual teacher requires either holding a three-year tertiary qualification, or a lower level qualification (upper secondary or short-cycle tertiary level) combined with relevant work experience. The requirements for becoming a tenured teacher are more stringent. Candidates must succeed at a centralised examination for vocational upper secondary teachers (CAPLP), in the case of cyber security the examination focuses on electrical engineering. Candidates must hold a short-cycle tertiary qualification (at least), and five years of relevant work experience either in industry or in teaching. As successful candidates become civil servants, employment outside the school is subject to strict regulation (Vocation Enseignant, 2023[62]).

Part-time teachers who pursue employment in the private sector while dedicating some time to teaching are more common in upper-secondary and higher education. The teacher workforce in tertiary education programmes includes full-time teachers (who hold the title teacher-researcher) and part-time teachers from industry. All providers of programmes that lead to cyber security professions report extensively using part-time teachers who are industry professionals. The precise share of full-time teachers vs. part-time industry professionals varies across providers and programmes. However, including industry professionals is also one of the evaluation criteria for engineering schools (evaluated by the "*Commission des titre d'ingénieur*"). This is viewed by providers as essential in linking the content of their programmes to rapidly changing industry needs.

There is some variation across providers in how easy it is for them to recruit industry professionals who are willing to work as part-time teachers. Salaries for part-time teaching are not competitive compared to what skilled professionals may earn in industry. At the same time, industry professionals have different motives for engaging with teaching. Some have decades of industry experience and seek to pursue a different type of professional engagement. Others have close links with a particular provider, for example because they are alumni or because they collaborate on a research project, so they accept to teach part-time. For provider institutions engagement with part-time teachers involves additional administrative tasks. For example, schedules need to be organised around the professional constraints of part-timers. In the area of cyber security, some professionals may be on call for emergency situations, so unexpectedly they may not be available for their usual lesson. Inevitably, some part-time teachers may quit teaching, so they need to be replaced from one year to another. New part-time teachers need extra support as they gain confidence in teaching a course.

For full-time teachers, applied research projects conducted jointly with industry are an important means of maintaining close connections with this fast-changing sector. The way teaching tasks are shared between full-time and part-time teachers also varies across institutions. Some institutions report that theoretical subjects are taught by full-time academics, while more applied courses are commonly taught by part-time teachers from the industry. Other providers report that subjects are shared between full-time and part-time teachers based on their particular expertise, not necessarily along these lines.

Multiple initiatives have been implemented to facilitate the participation of experts in the cyber security teaching workforce. One such initiative is led by Campus Cyber, a central hub for cyber security collaboration, where relevant stakeholders such as training providers and companies meet to exchange experiences and knowledge. For instance, experts from multiple cyber security organisations located on the campus participate as teachers at the School of Engineering and Computer Science, EPITA, which is also based on the campus (see Box 3.8).

Box 3.8. Campus Cyber: Bringing together cyber security stakeholders in one place

Campus Cyber is a comprehensive initiative aimed at establishing a central hub for cyber security expertise and collaboration. It involves more than 250 actors, including businesses, government entities, academia, and research institutions, and is driven by the French Government's vision to forge a cohesive cyber security ecosystem.

Key aspects of Campus Cyber:

- **Multi-Sector Collaboration:** Campus Cyber represents a national endeavour that integrates stakeholders from various sectors, emphasising the synergy between theoretical knowledge and practical application.
- **Educational Framework Development:** The initiative prioritises developing a robust educational framework to address the shortage of qualified cyber security educators. It aims to do this through partnerships with academic experts and leveraging technology for remote and scalable training solutions.
- **Cyber security occupation standards:** Cyber Campus training working group (which brings together the public and private players in the sector, including the MENJ) has worked on two innovative resources, which have been given the status of "cyber security commons", the skills matrices for technical occupations and related occupations in the cyber sector (Campus cyber, 2023[63]).

- **Work-Based Learning Opportunities:** Campus Cyber serves as a bridge between the educational sector and the industry, integrating practical experience into cyber security training programmes through internships, apprenticeships, and collaborative projects.
- **Consortium for Cyber security Talents:** Leading a consortium with educational institutions, associations, and mass media public companies, to increase attractiveness of the profession and change perceptions about cyber jobs, especially among young women and girls, and promoting cyber security as an attractive career option; provide educational guidance to encouraging students to engage in cyber security training and improving their awareness of cyber jobs and skills; and expand cyber training offerings to accommodate more students and make these programmes more relevant and attractive.
- **Addressing Teaching Workforce Challenges:** Campus Cyber dedicates spaces to cyber schools and integrates them into its governance system. This approach creates a link between schools and industry experts who can contribute teaching skills, lectures, and workshops.
- **Resources for Teacher Upskilling:** Specific online courses and workshops are designed by Campus Cyber and its partners to assist teachers in acquiring advanced cyber security skills.

By leveraging its unique position at the intersection of government, business, and education, Campus Cyber is set to play a pivotal role in shaping a new generation of cyber security experts. It underscores the importance of a dynamic and interactive learning environment that stimulates growth and innovation in France’s digital security sector. The initiative's comprehensive approach not only addresses current educational and workforce needs but also sets a foundation for long-term resilience and capability in the cyber security domain.

Source: Campus Cyber (2023[64]), concept: Réunir les acteurs de la sécurité numérique au sein d’un lieu totem pour protéger la société et faire rayonner l’excellence française du domaine, https://campuscyber.fr/.

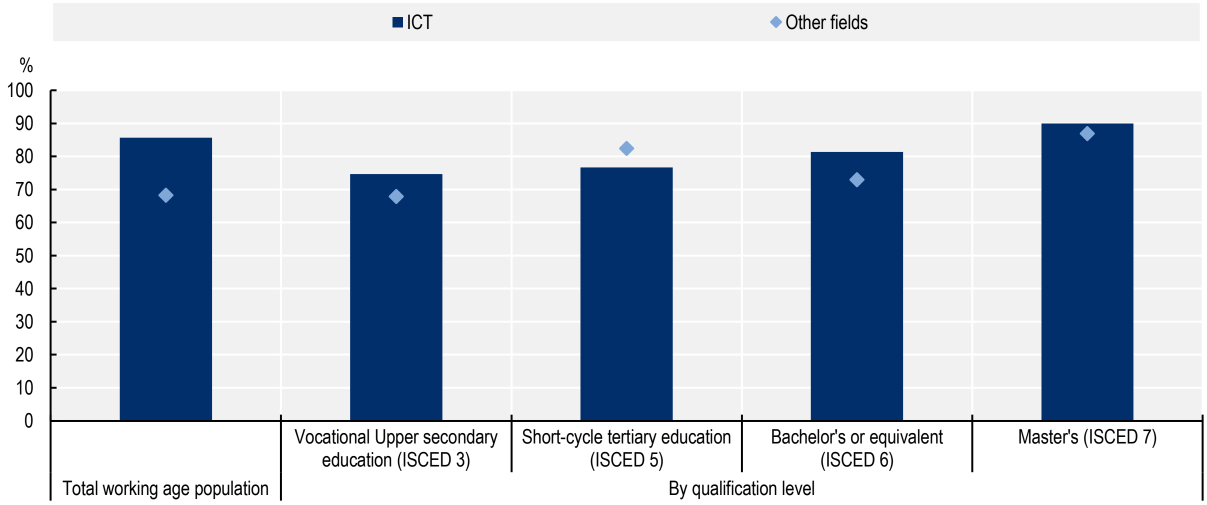
Labour market outcomes from cyber security education

Employability

Reflecting the increasing demand for cyber security professionals (see Chapter 2) individuals trained in cyber security are highly employable (BDM, 2022[65]). In general, ICT graduates have higher employment rate than graduates with qualifications at the same level from other fields. In 2020, in France, 86% of ICT graduates from across all levels of education were employed compared to 68% of graduates from other fields. Similar patterns are found by qualification level except for graduates with short-cycle tertiary degree (e.g. BUT), who have lower employment rate than those from other fields. This is mainly due to the fact employer consider cyber security roles often require specialised skills and certification beyond foundational knowledge, which demands candidates with more extensive training or higher educational qualification for roles that are more complex. As a consequence, ICT graduates with a master’s degree have the highest employability rate among all ICT professionals (90% in 2020). Moreover, most graduates with cyber security specialisation find employment within a few months of completing their education (Eurostat, 2022[66]).

Figure 3.12. Employment rate for ICT graduates versus other fields, by level of education, 2020

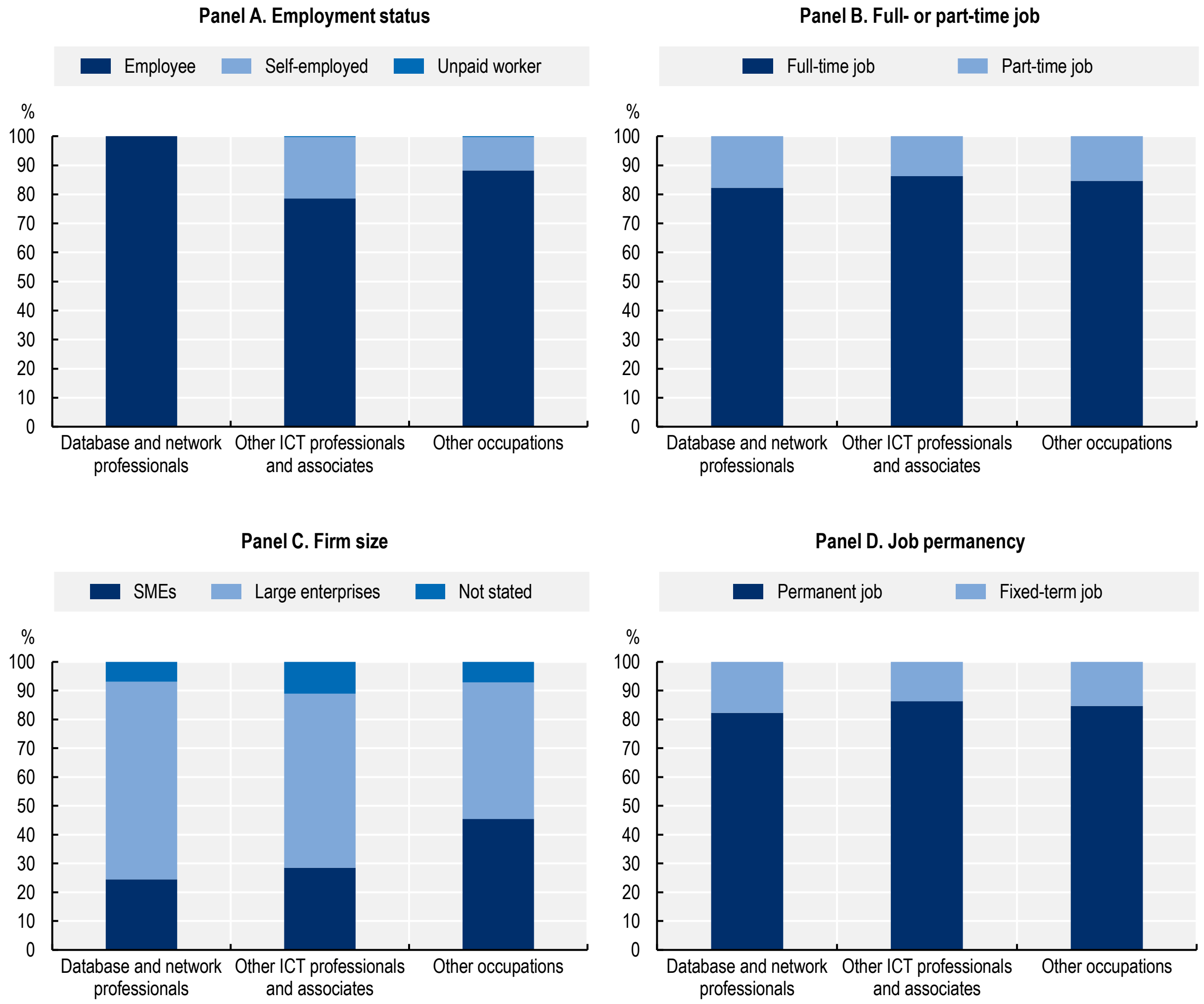
Percentage of the working-age population, by qualification level and field



Note: ICT includes all the individual that indicated holding a degree in the ICT, including those related to cyber security. Other fields do not include a field data related such as engineering, manufacturing and construction, health and others. The field of study information is gathered for individuals that indicate attained at least upper secondary education.
Source: OECD calculations using Labour Force Survey. Eurostat (2022[67]), EU Labour force survey, https://ec.europa.eu/eurostat/web/microdata/european-union-labour-force-survey.

The long-term job quality for cyber security professional in France are also favourable. Cyber security professionals work mostly as employee and mostly so for large enterprises (see Figure 3.13, Panel A and Panel C). The proportion of cyber security professionals working in large enterprises is higher (69%) than for other ICT professionals (60%). Job stability is a strong feature in this field, as cyber security experts are integral to the long-term digital strategy of organisation. 82% cyber security professionals work full time, which is slightly lower than in other ICT fields, but higher than for professionals outside of the ICT field (see Figure 3.13, Panel B). In terms of the contract, most of cyber security professionals have a permanent job contract (82%) (see Figure 3.13, Panel D). Furthermore, the versatile skills set acquired in cyber security education allows for career flexibility, enabling professional to change and adapt to new roles or specialisation as the field evolves.

Figure 3.13. Employment characteristics of database and network professionals compared to other ICT and other sectors professionals

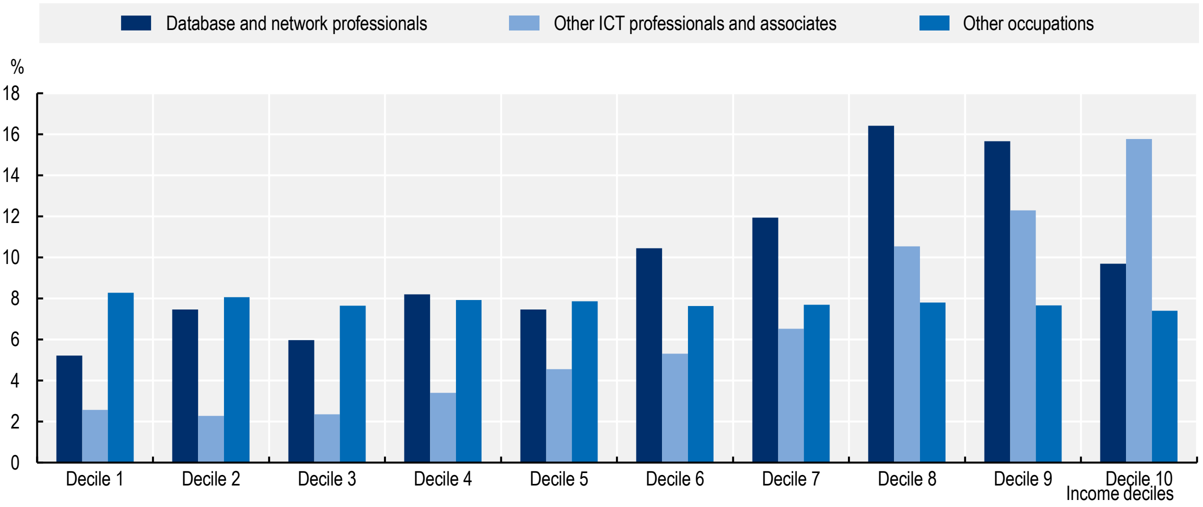


Note: Database and network professionals include cyber security professionals. Database and network professionals and other ICT professionals and associates include technicians, associate and professionals (including categories 2 and 3 of International Standard Classification of Occupations classification). Other occupation includes all the remaining categories of the ISCO classification, including professional and associates no in the ICT sector.
Source: OECD calculations using Labour Force Survey. Eurostat (2022[67]), EU Labour force survey, https://ec.europa.eu/eurostat/web/microdata/european-union-labour-force-survey.

Wages

Database and network professionals including those in cyber security earn higher incomes than their peers in other ICT roles and across other occupations (see Figure 3.14). Cyber security professionals predominantly occupy the higher income deciles. Cyber security skills are especially lucrative within the ICT sector, contrasting with a more uniform distribution of earnings among other cyber security jobs in sectors other than ICT. For instance, the average salary for a web and cyber security specialist in France is around EUR 75 996, with a range typically between EUR 58 121 and EUR 90 009. Similarly, a cyber security engineer's average salary is approximately EUR 68 025 in 2023 (Payscale, 2023[68]). For comparison, the average yearly salary for an information technology manager, which can be considered a broader ICT role, is around EUR 62 500 in France in 2023[1] (Salary explore, 2023[69]). These high salaries are primarily due to the increasing importance and complexity of safeguarding digital assets in the modern, digitally-driven world. It can also be attributed to the strong market demand for cyber security skills, coupled with a global shortage of qualified cyber security professionals, which further drive up their value and salaries.

Figure 3.14. Distribution of database and network professionals and other professionals by income deciles, 2020



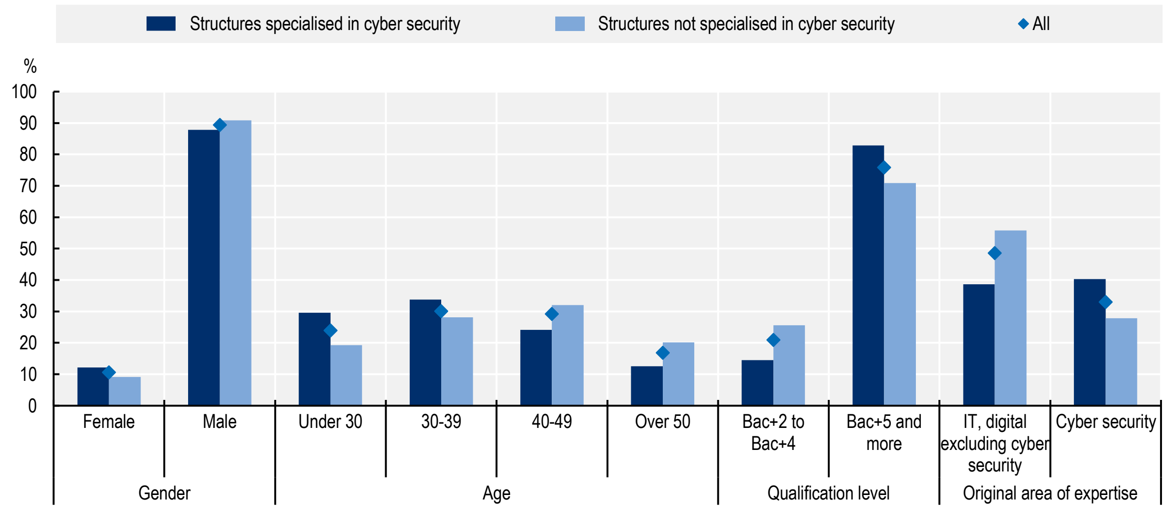
Note: Database and network professionals include cyber security professionals. Database and network professionals and other ICT professionals and associates include technicians, associate and professionals (including categories 2 and 3 of the International Standard Classification of Occupations classification). Other occupation includes all the remaining categories of the ISCO classification, including professional and associates no in the ICT sector.
Source: OECD calculations using Labour Force Survey. Eurostat (2022[67]), EU Labour force survey, https://ec.europa.eu/eurostat/web/microdata/european-union-labour-force-survey.

Diversifying the profile of cyber security professionals

The profile of cyber security learners and professionals

The typical cyber security professional in France is a highly qualified male between 30 to 49 years old, with specialised training in the IT/digital field, and with a bac+5 or higher education level (as shown in Chapter 2). However, the profession is getting younger, especially in most cyber security intensive occupations. A significant portion, 59%, of these professionals are aged between 30 and 49; 30% fall into the 30-39 bracket, while 29% are between 40 and 49 (see Figure 3.15). Notably, structures specialised in cyber security (i.e. organisations, departments or units that primarily provide specialising cyber security services and solutions)[2] tend to employ a higher percentage of professionals under 30. This trend can be largely attributed to the fact that younger professionals, being recent graduates, are more in tune with the latest trends, technologies, and best practices in cyber security.

Figure 3.15. Characteristics of cyber security professionals



Source: ANSSI (2022[70]) Les profils de la cybersécurité : Enquête 2021, www.ssi.gouv.fr/uploads/2021/10/anssi-les_profils_de_la_cybersecurite-enquete_2021.pdf.

Most of new entrants into the cyber security profession lack a formal education background in cyber security. This gap may be due to insufficient information and availability of targeted training opportunities. According to a 2021 ANSSI survey, 52% of cyber security professionals hold degrees in general computer science or related digital fields, while only 31% and 19% possess specialised cyber security degrees and cyber security certification, respectively (ANSSI, 2021[71]). Additionally, awareness of available training opportunities is relatively low, with just 44% of new entrants being cognisant of such opportunities (ANSSI, 2021[71]). To stay current, young professionals often rely on informal learning methods; 86% engage in self-study and 82% leverage their professional networks to update their cyber security skills.

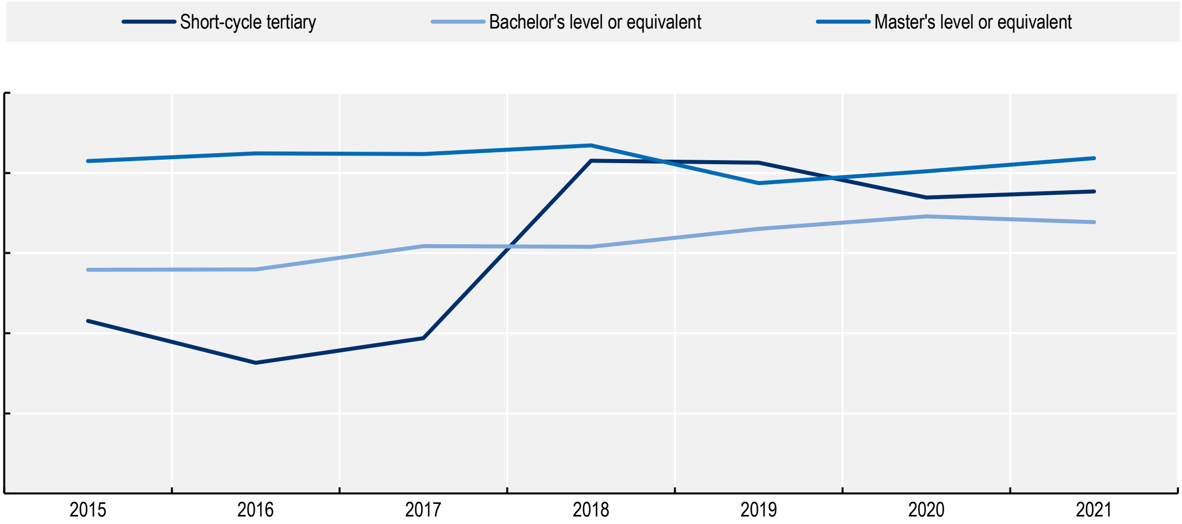
The professionals in cyber security are highly qualified, even at the start of their career. 76% of cyber security professionals hold a diploma or a level of qualification equal or greater than bac+ 5, which also reflects the labour market demand (see Chapter 2). Among the newcomers in the field, this proportion is slightly lower (72%). For cyber security professionals working within specialised cyber security sector (83%).

Females account for just 11% of cyber security professionals in France (BercyNumérique, 2023[72]). Interviews conducted with various institutions that deliver programmes preparing for cyber security suggest that the share of females among students is low, rarely exceeding 20%. Some providers reported that the share of females in cyber security education and training programmes had been growing but this improvement stopped as a result of COVID-19 related restrictions, which left limited room for career guidance interventions in schools.

This reflects the low levels of participation in ICT programmes among females in France, with around 20% of those graduating from ICT being females. The share of females among ICT graduates has been relatively stable at master's level. At bachelor's level there has been a slow increase over the past few years. At short-cycle tertiary level the share of females have increased strongly, from around 10% in 2015 to nearly 19% in 2021 (see Figure 3.16). Among OECD countries, a few have a higher share of females among ICT graduates – examples include Israel (53%), Norway (31%), Canada (28%) and Sweden (27%). At bachelor's level, the share of females among ICT graduates is similarly low: females accounted for 17% of graduates in 2021 in France. Over the past years, the share of females has been increasing among ICT bachelor's graduates, up from 14% in 2015. At this level as well, Israel and Sweden higher shares of females (31% and 35% respectively).

Figure 3.16. Trends in the share of females among ICT graduates in France

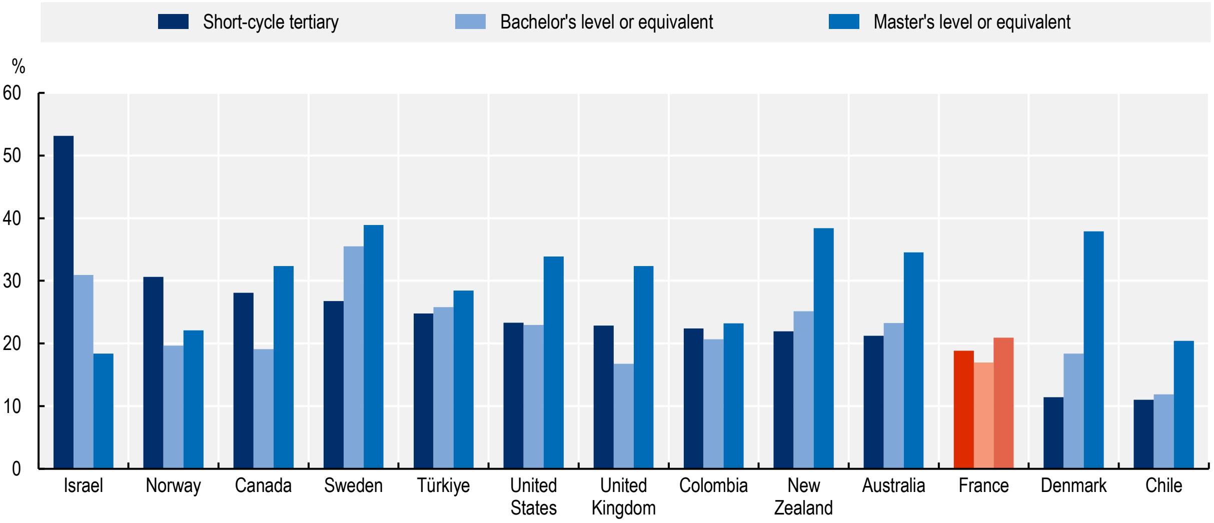
By level of tertiary education



Source: UOE data collection on education systems administered annually by UNESCO, the OECD and Eurostat.

Figure 3.17. The share of females among ICT graduates in selected OECD countries (2021)

By level of tertiary education



Source: UOE data collection on education systems administered annually by UNESCO, the OECD and Eurostat.

Inclusive language in cyber security job postings

French law stipulates that, except for certain occupations like models and actors, all jobs need to be explicitly addressed to both men and females (French Government, 2023[73]). Signalling that a job is open to men and females is most commonly done by including an expression like "H/F" to mean male/female,[3] or by using both gendered noun endings, for instance "Employé(e)" to mean both male and female employee.

The online job postings data provided by Lightcast contain a transcript of the job title that is mentioned for each job posting. This job title can be used to identify the type of language that is used in job postings to capture the attention of job seekers. In this context, leveraging the text available in the job titles can help make visible what kind of gendered language is used in job titles, as well as whether a job title explicitly mentions that the position is open to multiple genders.

To examine how inclusive French cyber security roles are to females,[4] this section performs a keyword analysis of 91 042 job titles in between January 2018 and June 2023 (see Annex 3.A) for more details on the method). First, the share of OJPs which includes an explicit gender signifier, so either "H/F" or a gendered noun ending, is calculated. Next, the share of OJPs for which a job title has both a feminine and a masculine variant is shown, as well as how many of these OJPs actually include the feminine variant of that title.[5]

In total, 86.1% of all cyber OJPs include a gender signifier in the job title, which means around one seventh of OJPs do not.[6] While this result does not immediately suggest that employers who omitted a gender signifier are inherently non-inclusive, the analysis does indicate that the absence of such a signifier could potentially point to a disregard or indifference towards promoting gender diversity and inclusion in the workplace. While it is essential not to overgeneralise, this lack of proactive gender representation may hint at underlying biases or challenges some employers face in promoting females in the cyber security profession.

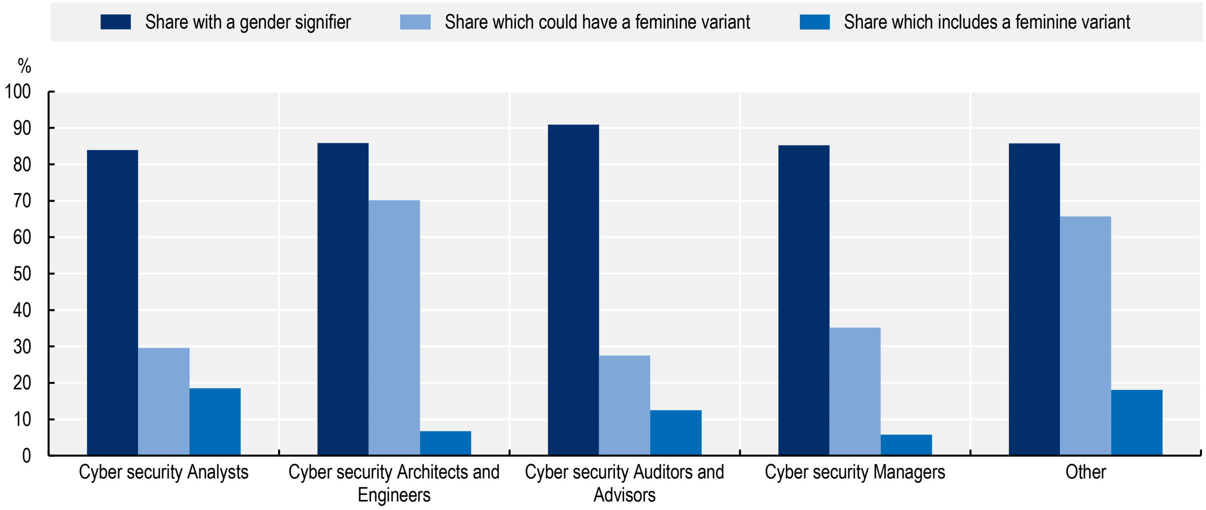
The feminisation of the names of professions has become increasingly more common in France in the last decade. For instance, in 2019 the *Académie française* published a report on this topic, in which they pronounced that in principle, from the perspective of the rules of the French language, there is no obstacle to the feminisation of professions (Académie française, 2019[74]).This was the first time that this influential institution, which was created in 1634, has gone this far in recognising the feminine in words (Rérolle, 2019[75]).

However, only around one-fifth of cyber security OJPs for which a feminine form exists actually includes the feminine form. In total there are around 54% of OJPs for which both a feminine and a masculine form of the role exist, the other OJPs are for roles like "Analyste" or "Juriste", which do not have a gendered noun ending. Jobs which do have the potential for a feminine form are roles like developer (*développeuse/développeur*), administrator (*administratrice/administrateur*), and manager (*cheffe/chef*) for example.

The fact that a low share of OJPs makes use of feminine noun endings, combined with 14% of OJPs which do not include any gender signifiers, shows that there is still room for promoting more inclusivity in the cyber security field, starting from the use of more inclusive language when looking for potential candidates to hire. The data cannot show whether there are objective barriers for females to enter into cyber security professions, but there is an indication that many employers do not think about the explicit inclusion of females in this technical field.

Figure 3.18 shows that the results differ significantly per cyber security job role, especially with respect to opting to use a gendered noun ending. The share of OJPs including any type of gender signifier in the job title ranges between 84% for cyber security analysts, to 91% for auditors and advisors. For cyber security analysts, a feminine variant of the profession only exists for a third of job titles, however, in nearly two thirds of those cases, the employers opt to include this feminine variant. By contrast, for the roles which are most focused on programming and informatics, architects and engineers, a feminine version of the job role exists around 70% of the time, however, in only 7% of these OJPs the feminine variant is actually mentioned. In total, 86% of OJPs for this role still include a gender signifier, so most use “H/F”. The results therefore show, a discrepancy in the use of feminine variant of the profession between the different job roles, as evidenced by for instance architects and engineers compared to analysts.

Figure 3.18. Gender signifiers per cyber security job role



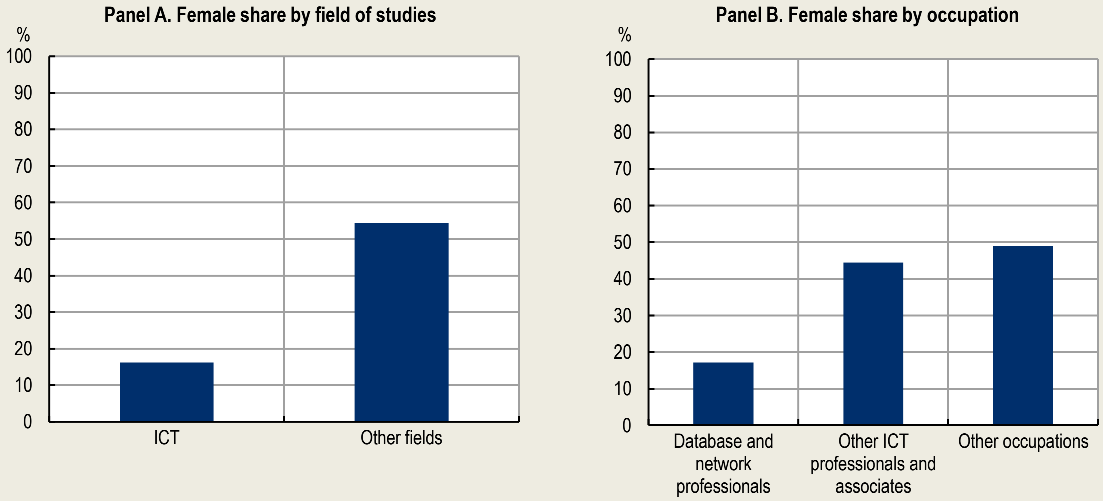
Source: OECD calculations based on Lightcast data.

The lack of gender diversity in cyber security education enrolment can be extrapolated to occupations. In France, the proportion of cyber security professionals who are females is notably low, mirroring the wider trend in the ICT sector (see Box 3.9).

Box 3.9. Females in the cyber security sector

Despite the French Government’s efforts to diversify the cyber security workforce, as discussed earlier in this chapter, females continue to be underrepresented in this sector, similar to the broader ICT sector. The proportion of females holding degrees in the ICT field is significantly lower compared to other fields. Currently, only 16% of ICT graduates in France are females, which is 38 percentage points less than in other fields (54%) (See Figure 3.19, Panel A). Furthermore, the share of females working as cyber security professionals (categorised under 'Database and network professionals’) is just 17%. This figure is substantially lower than their representation in other ICT occupations (44%) and even lower than in other occupations (49%) (see Figure 3.19, Panel B). The lack of diversity and gender parity has negative implications for cyber security organisations, not only because it widens their skills gaps but also because it restricts the range of perspectives on cyber-security, increasing the risk of business blind spots. Diverse teams, consisting of members with varied backgrounds and education, can offer a more comprehensive and well-rounded understanding of the specific needs of a business.

Figure 3.19. Females with an ICT degree or working in ICT occupations in 2022



Note: For Panel A. ICT includes all the individual that indicated holding a degree in the ICT, including those related to cyber security. Other fields do not include a field data related such as engineering, manufacturing and construction, health and others. The field of study information is gathered for individuals that indicate attained at least upper secondary education. For Panel B, database and network professionals include cyber security professionals. Database and network professionals and other ICT professionals and associates include technicians, associate and professionals (including categories 2 and 3 of the International Standard Classification of Occupations (ISCO) classification). Other occupations includes all the remaining categories of the ISCO classification, including professionals and associates not in the ICT sector.

Source: OECD calculations using Labour Force Survey. Eurostat (2022[67]), EU Labour force survey, https://ec.europa.eu/eurostat/web/microdata/european-union-labour-force-survey.

Initiatives to increase gender and socio-economic diversity

Diversifying the profile of cyber security professionals is seen as a key objective in France for various reasons. First, it allows to expand the talent pool, needed to reach the target of 75 000 individuals trained in cyber security by 2025. Second, having a diversity of perspectives among professionals is essential for effective cyber security strategies. Successful attacks rely on weaknesses that attackers have identified and professionals in the company have missed or have not addressed. A greater diversity of perspectives within a company is viewed as helpful in identifying and addressing such weaknesses. This section focuses on two aspects of diversity: gender and socio-economic background.

Box 3.10. Promoting females' participation in cyber security

Les Cadettes de la Cyber

Cyber Cadettes is a programme of the Cyber Excellence Centre launched in 2021. It aims to encourage young females to pursue a career in cyber security. It has various components:

- Mentorship: Each cadette has a mentor, who is a key figure in the cyber eco-system. She will have the opportunity to discuss career plans with her mentor, who monitors the progression of their mentee through individual coaching and facilitating access to their professional network.

- Training: The cadettes benefit from a range of training opportunities, including courses on cyber geopolitics, managerial training, and public speaking. Cadettes take the common core of the training programme together – this is at the heart of the training programme.
- Transition into jobs: The cadettes pursue internships in their area of expertise. The programme also includes job dating sessions and individualised job coaching.
- Media coverage: The cadettes act as ambassadors of the programme. They receive media training sessions, represent the programme at prestigious events (e.g. European Cyber Week, International Cyber security Forum) and are active on social media.

CEFCYS - Cercle des Femmes de la Cybersécurité

This association aims to promote the presence and leadership of females in cyber security professions. It has over 400 members (both females and men who work in the field), as well as those aspiring to work in cyber security. CEFCYS is active in six major cities in France (Paris, Lyon, Toulouse, Lille, Rennes, Marseille), as well as abroad (Argentina, Morocco, the Netherlands and Spain). Its activities include:

- Mentoring
- Masterclasses
- Raising awareness
- Training.

Women4Cyber France

Women4Cyber France, established in 2021, is an association representing the Brussels-based European Foundation Women4Cyber. It aims to address the gender imbalance in the cyber world, with two primary objectives: promoting women's participation in cyber professions and encouraging the field of cyber security to women. Recognising the male-dominated nature of the cyber environment, which impacts skill development, the economy, and national sovereignty, Women4Cyber France focuses on uniting both women and men engaged in cyber skills challenges. It strives to create a supportive network and raise awareness about cyber professions, contributing to a broader collective effort.

Source: Les cadettes de la cyber (2021[76]), Les Cadettes de la Cyber est un programme du Pôle d'Excellence Cyber (PEC), https://les-cadettes-de-la-cyber.org/; Cercle des femmes de la cybersecurite (2023[77]), Présentation : L'association des femmes de la Cybersécurité, https://cefcys.fr/association-femmes-cybersecurite/. Women4Cyber (2023[78]), women4Cyber European cyber security Organisation, https://women4cyber.eu/about-us/.

To combat the notable underrepresentation of females in France's cyber security sector, strategies like "Les Cadettes de la Cyber" and the "CEFCYS" association have been implemented (see Box 3.10). These initiatives not only aim to diversify the talent pool in cyber security but also to enhance the field's innovation and problem-solving capacity by integrating diverse perspectives essential for tackling complex cyber threats. Additionally, French Government has implemented campaigns in high schools and universities aim to encourage more women to pursue engineering and computer science studies (TechCrunch, 2017[79]). The initiative also supports companies in hiring more women, assists women in starting companies, and aids in job placement in tech companies. These efforts are part of a broader strategy to increase female participation in the cyber security sector in France, recognising the need for diverse perspectives in tackling complex cyber threats.

Beyond improving gender diversity, efforts have been focused on providing information about the various cyber security roles to expand young people's understanding of the field and its occupations. Recently the Ministry of Education and Youth (MENJ) has launched a campaign aims to introduce and attract a diverse range of young students' cyber security careers (see Box 3.11). By providing educational resources, showcasing a variety of roles within the sector, and engaging students in interactive learning experiences, the initiative seeks to break down stereotypes and promote cyber security as a viable and exciting career path, thereby helping to secure France's digital future.

Box 3.11. Breaking down the stereotypes of roles in cyber security

The “DemainSpécialisteCyber” national campaign, initiated by the ANSSI, the Ministry of National Education and Youth, and the Campus Cyber, is aimed at introducing middle and high school students to the field of cyber security. This campaign addresses the critical challenge of filling the cyber security skills gap in France by dismantling sector stereotypes and attracting more youth to this field.

The campaign encompasses various components including an informational website with educational resources, posters highlighting different cyber security professions, the “CyberEnJeux” hackathons, a TV spot, and interactive platforms like The Osint Project and PIX Cyber, which promote digital competency learning. Integrated into the career discovery programme for students from 5th to 9th grade, it receives support from several institutions and organisations, enhancing its effectiveness and reach.

The Minister of National Education and Youth emphasises the campaign’s significance in making cyber security professions known, especially among young girls, and contributing to France’s future sovereignty in this crucial economic sector. The campaign not only raises awareness but also inspires vocations in a field that is increasingly central to national security and the digital economy.

Source: MENJ (2023[80]), Lancement de la campagne nationale "DemainSpécialisteCyber" pour faire découvrir la cybersécurité et ses métiers, www.demainspecialistecyber.fr/.

Efforts to increase socio-economic diversity among cyber security professionals focus on ensuring that cyber security education is available in the types of programmes that enroll students from diverse backgrounds, and that those are linked to strong progression pathways to higher levels of education.

Upper secondary programmes play an important role in diversifying the socio-economic background of future cyber security professionals. They have the potential to develop technical skills relevant to cyber security among students from less privileged socio-economic backgrounds. Programmes leading to the Vocational or Technological Baccalaureate tend to enrol, on average, more students from disadvantaged backgrounds that programmes leading to the General Baccalaureate. For example, in 2020, children of parents who were managers or held a highly skilled profession accounted for a third of those who obtained the General Baccalaureate. Their share among Technological or Vocational Baccalaureate was much lower (16% and 8% respectively) (MENJ, 2023[81]). In addition, these programmes (and in particular the Technological Baccalaureate) can serve as an entry route into higher education programmes in cyber security.

Higher education programmes delivered in University Institutes of Technology (including BTS, BUT and professional bachelor’s programmes) have the potential to play an important role in terms of diversifying the social background of future cyber security professionals.

First, they provide a progression route for graduates of the Vocational or Technological Baccalaureate, Quotas have been implemented to facilitate such transitions. For BTS programmes the quota varies, but Vocational and Technological Baccalaureate graduates account for around two-thirds of all BTS entrants (32% and 30% respectively, data for cyber security only were not available) (Letudiant, 2023[82]). Graduates of the Vocational Baccalaureate (either “Cyber security, IT, networks, electronics” or “Electricity and connected environments”) or Technological Baccalaureate (Sciences and technologies of Industry and sustainable development”) can transition relatively easily into a BTS in “Cyber security, IT and networks, electronics". On the other hand, in BUT programmes half of available places are reserved for graduates of a Technological Baccalaureate within a related field. Those who obtained a Technological Baccalaureate with excellent results (*mention bien* or *très bien*) are automatically admitted (ONISEP, 2023[83]). In the case of cyber security, for example, there is a progression route for graduates of a Technological Baccalaureate in "Sciences and technologies of Industry and sustainable development" into a BUT in "Networks and telecommunications".

More broadly, the socio-economic background of entrants to BTS and BUT programmes (all fields included) is more diverse than that of scientific preparatory courses, which are the classical entry route into engineering schools. Data from the 2017 admission process show that those admitted to a scientific preparatory course had a very high share of students from privileged backgrounds and one of the highest shares of excellent results at the baccalaureate (INSEE, 2021[84]). BTS and BUT (formerly DUT) programmes on the other hand, have a more diverse student intake. 17% of BTS entrants have excellent results at the baccalaureate and around 30% come from privileged backgrounds. DUT programmes had 28% of their entrants with excellent results at the baccalaureate and around half from privileged backgrounds.

Professional bachelor's degrees, which include a range of programmes with SecNumEdu certification, in turn allow BTS and year 2 BUT graduates to further their technical skills and obtain a bachelor's qualification. Given the admission routes to these programmes, the socio-economic profile of professional bachelor's students will also be more diverse than that of preparatory courses and engineering schools.

Finally, upon completion of a part or the entirety of a programme within a University Institute of Technology, students may transition into an engineering school. A growing number of engineering schools admit such students. The share of BTS or BUT graduates among entrants to engineering programmes varies from around half of entrants in some schools, to just a few or no entrants at all. On average 18.5% of those admitted to engineering schools are graduates of a BTS or BUT programme and 8% have completed the second or third year of a bachelor's programme (ONISEP, 2022[85]). To facilitate successful transitions from practically oriented programmes to more theoretical, research-oriented engineering programmes, BTS graduates may pursue a bridging year ("higher technician adaptation", *adaptation technicien supérieur*).

References

Académie française (2019), *La Féminisation des Noms de Métiers et de Fonctions*, https://www.academie-francaise.fr/sites/academie-francaise.fr/files/rapport_feminisation_noms_de_metier_et_de_fonction.pdf (accessed on 1 October 2023). [74]

ANR (2021), *Compétences et Métiers d'Avenir (CMA) – Appel à manifestation d'intérêt – 2021-2025*, https://anr.fr/fr/detail/call/competences-et-metiers-davenir-cma-appel-a-manifestation-dinteret-2021-2025/. [49]

ANSSI (2023), *FORMATIONS CONTINUES LABELLISÉES SECNUMEDU-FC*, https://www.ssi.gouv.fr/particulier/formations/secnumedu-fc-labellisation-de-formations-continues-en-cybersecurite/formations-continues-labellisees-secnumedu/. [45]

ANSSI (2023), *Se former à la cybersécurité*, https://cyber.gouv.fr/se-former-la-cybersecurite. [57]

ANSSI (2022), *Les profils de la cybersécurité: Enquête 2021*, https://www.ssi.gouv.fr/uploads/2021/10/anssi-les_profils_de_la_cybersecurite-enquete_2021.pdf. [70]

ANSSI (2021), *France Relance*, https://www.ssi.gouv.fr/agence/cybersecurite/france-relance/le-volet-cybersecurite-de-france-relance-faq/. [2]

ANSSI (2021), *Les professionnels de 5 ans et moins d'expérience dans le domaine de la cybersécurité (The professionals 5 years and under of experience in the field of cyber security)*, https://www.ssi.gouv.fr/uploads/2021/10/zoom_5_ans_experience_ou_moins_mars22_v3.pdf. [71]

ANSSI (2020), *Panorama des métiers de la cybersécurité*, https://www.ssi.gouv.fr/uploads/2021/10/anssi-panorama_metiers_cybersecurite-2020.pdf. [1]

BDM (2022), *Cybersécurité : l'APEC dresse le panorama de l'emploi cadre en 2022*, https://www.blogdumoderateur.com/cybersecurite-apec-dresse-panorama-emploi-cadre-2022/. [65]

BercyNumérique (2023), *Cybersécurité : vers une parité hommes-femmes du secteur ?*, https://www.bercynumerique.finances.gouv.fr/cybersecurite-vers-une-parite-hommes-femmes-du-secteur. [72]

Campus cyber (2023), *concept: Réunir les acteurs de la sécurité numérique au sein d'un lieu totem pour protéger la société et faire rayonner l'excellence française du domaine*, https://campuscyber.fr/. [64]

Campus cyber (2023), *Matrice des compétences des métiers techniques*, https://wiki.campuscyber.fr/Matrice_des_comp%C3%A9tences_des_m%C3%A9tiers_techniques. [63]

Cercle des femmes de la cybersecurite (2023), *Présentation: L'association des femmes de la Cybersécurité*, https://cefcys.fr/association-femmes-cybersecurite/. [77]

CESI (2023), *Bachelor en sciences et en ingenierie*, http://www.cesi.fr/programmes/cycle-bachelor-en-sciences-et-en-ingenierie/. [36]

CNAM Paris (2023), *Certificat de compétence Analyste en cybersécurité*, https://www.cnam-paris.fr/certificat-de-competence-analyste-en-cybersecurite-1263707.kjsp. [41]

Couppié, T. and C. Gasquet (2021), *Débuter en CDI : le plus des apprentis*, https://www.cereq.fr/debuter-en-cdi-le-plus-des-apprentis. [58]

CyberEdu (2022), *Le project*, https://www.cyberedu.fr/pages/le-projet/. [52]

DEPP (2023), *Repères et références statistiques, edition 2023*, https://www.education.gouv.fr/reperes-et-references-statistiques-2023-378608. [9]

DEPP (2016), *Repères and références statistiques*, https://www.education.gouv.fr/sites/default/files/imported_files/document/depp_rers_2016_614975.pdf. [61]

Depp (2022), *Repères et références statistiques 2022*, https://www.education.gouv.fr/media/116557/download. [7]

Depp (2012), *Repères et réferences statisques sur les enseignements, la formation et la recherche, 2012*, https://cache.media.enseignementsup-recherche.gouv.fr/file/2012/06/4/DEPP-RERS-2012_224064.pdf. [8]

ECE (2023), *Bachelor en cybersécurite*, http://www.ece.fr/faq/bachelor-cybersecurite/. [32]

Education (2023), *Le baccalauréat technologique*, https://www.education.gouv.fr/reussir-au-lycee/le-baccalaureat-technologique-1916. [16]

EDUSCOL (2023), *Rénovation de la filière systèmes numériques en " Cybersécurité, Informatique et réseaux, Electronique (CIEL)*, https://eduscol.education.fr/sti/actualites/renovation_filiere_ciel. [14]

ENISA (2022), *European Cybersecurity Skills Framework (ECSF)*, https://www.enisa.europa.eu/topics/education/european-cybersecurity-skills-framework. [51]

EP (2023), *Executive MSc in Cybersecurity*, http://www.ip-paris.fr/en/education/lifelong-learning/executive-msc-cyber security. [39]

EPITA (2023), *Bachelor en cybersécurité*, http://www.epita.fr/bachelor-cybersecurite/. [33]

ESAIP (2023), *Bachelor en ingenierie informatique et cybersécurité*, https://www.esaip.org/formation/bachelor-en-ingenierie-informatique-et-cybersecurite/. [34]

ESAIP (2023), *Bachelor numerique*, http://www.esaip.org/formation/bachelor-numerique/. [35]

Eurostat (2022), *EU labour force survey*, https://ec.europa.eu/eurostat/web/microdata/european-union-labour-force-survey. [67]

Eurostat (2022), *ICT education - a statistical overview*, https://ec.europa.eu/eurostat/statistics-explained/index.php?oldid=454538#:~:text=In%20the%20EU%2C%20more%20than,ICT%20educated%20persons%20are%20employed. [66]

French Government (2023), *Offre d'emploi et embauche : les droits du candidat*, https://travail-emploi.gouv.fr/droit-du-travail/la-vie-du-contrat-de-travail/article/offre-d-emploi-et-embauche-les-droits-du-candidat (accessed on October 2023). [73]

GOuvernement (2021), *Un plan à 1 milliard d'euros pour renforcer la cybersécurité*, https://www.gouvernement.fr/actualite/un-plan-a-1-milliard-d-euros-pour-renforcer-la-cybersecurite. [48]

Gouvernement (2023), *Maitriser les technologies numériques souveraines et sûres*, https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2023/07/levier_maitriser_les_technologies_numeriques_ok_ov_ajout_ensnum_verdissement_ok.pdf. [3]

INSA (2023), *Computer security and technologies (STI)*, http://www.insa-centrevaldeloire.fr/en/training/Information-technology-and-cyber security. [38]

INSA Lyon (2023), *Cybersécurité du Numérique*, https://www.insa-lyon.fr/fr/mastere-cybersecurite-numerique. [40]

INSEE (2021), *France, portrait social*, https://www.insee.fr/fr/statistiques/5432519?sommaire=5435421#tableau-figure2_radio1. [84]

IUT Haguenau (2023), *Systemes automatises, reseaux et informatique industrielle*, https://iuthaguenau.unistra.fr/formations/licence-pro/systemes-automatises-reseaux-et-informatique-industrielle. [55]

IUT La Rochelle (2023), *BUT informatique*, http://www.iut-larochelle.fr/formations/departement-informatique/but-informatique/. [29]

IUT Valence (2023), *BUT informatique*, https://www.iut-valence.fr/nos-formations/b-u-t-/b-u-t-info/b-u-t-informatique-776395.kjsp. [30]

IUT Ville d'Avray Saint-Cloud Nanterre (2023), *Licence professionnelle i2ap*, https://cva-geii.parisnanterre.fr/formations/licence-professionnelle-i2ap. [56]

JORF (2023), *Arrêté du 25 janvier 2023 portant définition et fixant les conditions de délivrance du brevet de technicien supérieur « Cybersécurité, Informatique et réseaux, Electronique, option A : "Informatique et réseaux", option B : "Electronique et réseaux"*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047226070. [11]

JORF (2020), *Arrêté du 17 janvier 2020 accordant la reconnaissance par l'Etat à des écoles techniques privées pour des formations préparant au brevet de technicien supérieur pour la rentrée universitaire 2020*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000041477788. [5]

Leptidigital (2023), *Les Meilleures Plateformes en Ligne de Formation dans le Digital*, https://www.leptidigital.fr/internet/meilleures-plateformes-en-ligne-formation-digital-16991/. [46]

Les Cadettes de la Cyber (2021), *Les Cadettes de la Cyber est un programme du Pôle d'Excellence Cyber (PEC)*, https://les-cadettes-de-la-cyber.org/qui-sommes-nous/. [76]

Letudiant (2023), *Parcoursup : malgré les quotas de bacs pro, des places à prendre pour les bac généraux en BTS*, https://www.letudiant.fr/etudes/btsdut/parcoursup-malgre-les-quotas-de-bacs-pro-des-places-a-prendre-pour-les-bac-generaux-en-bts.html#:~:text=Explications.,106%20sp%C3%A9cialit%C3%A9s%20propos%C3%A9es%20en%20BTS. [82]

MENJ (2023), *Baccalauréat professionnel: Cybersécurité, Informatique et réseaux, Électronique (CIEL)*, https://eduscol.education.fr/sti/sites/eduscol.education.fr.sti/files/actualites/15324/15324-ref-bcp-ciel-vpub-eduscol.pdf. [10]

MENJ (2023), *Lancement de la campagne nationale "DemainSpécialisteCyber" pour faire découvrir la cybersécurité et ses métiers*, https://www.demainspecialistecyber.fr/. [80]

MENJ (2023), *Mention complémentaire de niveau 4*, https://eduscol.education.fr/sti/sites/eduscol.education.fr.sti/files/actualites/15324/15324-ref-mc-cyber-vpub-eduscol.pdf. [12]

MENJ (2023), *Réussir au lycée*, https://www.education.gouv.fr/reussir-au-lycee/le-baccalaureat-technologique-1916. [17]

MENJ (2023), *Réussite au baccalauréat selon l'origine sociale*, https://data.education.gouv.fr/explore/dataset/fr-en-reussite-au-baccalaureat-origine-sociale/table/?disjunctive.annee. [81]

MENJS (2023), *Réussir au lyceé*, https://www.education.gouv.fr/reussir-au-lycee/le-baccalaureat-technologique-1916. [20]

MESR (2023), *Arrêté du portant définition et fixant les conditions de délivrance du brevet de technicien supérieur - Cybersécurité, Informatique et résaux, Électronique*, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000047226070. [6]

MESR (2023), *Portant définition et fixant les conditions de délivrance du brevet de technicien supérieur "Cybersécurité, Informatique et réseaux, Électronique, Option A et Option B"*, https://enqdip.sup.adc.education.fr/bts/referentiel/BTS_Cybersecurite_Informatique_reseaux_electronique.pdf. [22]

MESR (2022), "Note d'information du SIES", in *Les effectifs d'étudiants dans le supérieur continuent leur progression en 2021-2022*, https://www.enseignementsup-recherche.gouv.fr/fr/les-effectifs-d-etudiants-dans-le-superieur-continuent-leur-progression-en-2021-2022-88609. [26]

MESR (2022), *Licence professionnelle*, https://www.enseignementsup-recherche.gouv.fr/fr/licence-professionnelle-45883#:~:text=Accessible%20auparavant%20apr%C3%A8s%20un%20bac%2B,tout%20moment%20du%20premier%20cycle. [31]

MFIDS (2022), *Stratégie nationale d'accélération pour la cybersécurité : les premières réalisations*, https://www.economie.gouv.fr/strategie-nationale-acceleration-cybersecurite. [43]

MFIDS (2021), *Cybersécurité : renforcement par le Gouvernement de la protection des citoyens, des administrations et des entreprises*, https://www.economie.gouv.fr/cybersecurite-renforcement-gouvernement-protection-citoyens-administrations-entreprises. [44]

MTPEI (2021), *Employeurs, recrutez en alternance : une solution pour l'avenir de votre entreprise*, https://travail-emploi.gouv.fr/actualites/l-actualite-du-ministere/article/employeurs-recrutez-en-alternance-une-solution-pour-l-avenir-de-votre. [27]

MTPEI (2017), *Certificat de Qualification Professionnelle (CQP)*, https://travail-emploi.gouv.fr/formation-professionnelle/certification-competences-pro/article/certificat-de-qualification-professionnelle-cqp. [47]

NSI (2023), *La semaine du numérique et des sciences informatiques*, https://www.semaine-nsi.fr/. [25]

ONISEP (2023), *Bac pro cybersécurité, informatique et réseaux, électronique (CIEL)*, https://www.onisep.fr/ressources/univers-formation/formations/Lycees/bac-pro-cybersecurite-informatique-et-reseaux-electronique. [13]

ONISEP (2023), *BTS cybersécurité, informatique et réseaux, électronique option B électronique et réseaux (CIEL ER)*, https://www.onisep.fr/ressources/univers-formation/formations/Post-bac/bts-cybersecurite-informatique-et-reseaux-electronique-option-b-electronique-et-reseaux. [21]

ONISEP (2023), *Le bac STMG (sciences et technologies du management et de la gestion)*, https://www.onisep.fr/formation/apres-la-3-la-voie-generale-et-technologique/qu-est-ce-que-la-voie-generale-et-technologique/la-voie-technologique-en-premiere-et-terminale/le-bac-stmg-sciences-et-technologies-du-management-et-de-la-gestion. [18]

ONISEP (2023), *Les BUT (Bachelors universitaires de technologie*, https://www.letudiant.fr/etudes/btsdut/parcoursup-malgre-les-quotas-de-bacs-pro-des-places-a-prendre-pour-les-bac-generaux-en-bts.html#:~:text=Explications.,106%20sp%C3%A9cialit%C3%A9s%20propos%C3%A9es%20en%20BTS. [83]

ONISEP (2023), *Les BUT (bachelors universitaires de technologie)*, https://www.onisep.fr/formation/apres-le-bac-les-etudes-superieures/les-principales-filieres-d-etudes-superieures/les-but-bachelors-universitaires-de-technologie#:~:text=Le%20BUT%20correspond%20%C3%A0%20180,de%20leurs%20deux%20premi%C3%A8res%20ann%C3%A9es. [28]

ONISEP (2023), *Les familles de métiers en seconde professionnelle*, https://www.onisep.fr/formation/apres-la-3-la-voie-professionnelle/les-diplomes-de-la-voie-pro/le-bac-professionnel/les-familles-de-metiers. [15]

ONISEP (2023), *Les stages en lycée professionnel*, https://www.onisep.fr/vers-l-emploi/stages-en-entreprises/les-stages-par-niveau-d-etudes/les-stages-en-lycee-professionnel. [59]

ONISEP (2023), *L'offre de formations de cybersécurité*, https://www.onisep.fr/recherche?context=formation&not_query_type=true&page=1&text=cybers%C3%A9curit%C3%A9. [4]

ONISEP (2022), *La voie technologique en première et terminale*, https://www.onisep.fr/formation/apres-la-3-la-voie-generale-et-technologique/qu-est-ce-que-la-voie-generale-et-technologique/la-voie-technologique-en-premiere-et-terminale. [19]

ONISEP (2022), *Les différentes voies d'accès en école d'ingénieurs*, https://www.onisep.fr/formation/les-principaux-domaines-de-formation/les-ecoles-d-ingenieurs/les-differentes-voies-d-acces-en-ecole-d-ingenieurs. [85]

ONISEP (2022), *Les stages dans l'enseignement supérieur*, https://www.onisep.fr/vers-l-emploi/stages-en-entreprises/les-stages-par-niveau-d-etudes/les-stages-dans-l-enseignement-superieur. [60]

Onisep (2023), *SISR*, https://www.onisep.fr/ressources/univers-formation/formations/Post-bac/bts-services-informatiques-aux-organisations-option-a-solutions-d-infrastructure-systemes-et-reseaux. [24]

Onisep (2023), *SLAM*, https://www.onisep.fr/ressources/univers-formation/formations/Post-bac/bts-services-informatiques-aux-organisations-option-b-solutions-logicielles-et-applications-metiers. [23]

Payscale (2023), *Average Cyber Security Engineer Salary in France*, https://www.payscale.com/research/FR/Job=Cyber_Security_Engineer/Salary. [68]

Rennes SB (2021), *Rennes School of Business ouvre son nouveau parcours « Global Tech & Cybersecurity »*, https://www.rennes-sb.fr/programmes-fr/nouveau-parcours-global-tech-cybersecurity-programme-grande-ecole/. [50]

Rérolle, R. (2019), *L'Académie française se résout à la féminisation des noms de métiers*, https://www.lemonde.fr/societe/article/2019/02/28/l-academie-francaise-se-resout-a-la-feminisation-des-noms-de-metiers_5429632_3224.html (accessed on October 2023). [75]

Salary explore (2023), *Salaries in France by occupation and sector*, https://www.salaryexplorer.com/average-salary-wage-comparison-france-c74. [69]

TechCrunch (2017), *French Government to promote gender equality in the tech ecosystem*, https://techcrunch.com/2017/01/31/french-government-to-promote-gender-equality-in-the-tech-ecosystem/?guccounter=1. [79]

TELECOM SudParis (2023), *Certification professionnelle à la Gouvernance de la sécurité des systèmes d'information et des réseaux*, https://www.telecom-sudparis.eu/formation/ces-securite-des-systemes-information-et-reseaux/. [42]

TELECOM SudParis (2023), *Sécurité des systèmes et des réseaux*, http://www.telecom-sudparis.eu/formation/securite-des-systemes-et-des-reseaux/. [37]

Université de Toulon (2023), *Licence informatique parcours informatique*, https://www.univ-tln.fr/Licence-Informatique-parcours-Informatique.html. [54]

UPEC (2023), *Licence economie et gestion parcours informatique et management*, https://www.u-pec.fr/fr/formation/niveau-l/licence-economie-et-gestion-parcours-informatique-et-management-miage. [53]

Vocation Enseignant (2023), *Professeurs certifiés de lycée professionnel : tendance de recrutement*, https://vocationenseignant.fr/reussir-le-concours-caplp-professeur-lycee-professionnel/. [62]

Women4Cyber (2023), *Women4Cyber European Cyber Security Organisation*, https://women4cyber.eu/about-us/. [78]

Annex 3.A. Classifying inclusive language in cyber security job postings using job titles

The online job postings data provided by Lightcast contain a transcript of the job title that is mentioned for each job posting. Leverageing the text available in the job titles can help make visible what kind of gendered language is used in job titles, as well as whether a job title explicitly mentions that the position is open to multiple genders. For this purpose, this report uses a classification strategy based on regular expressions, as in Annex 2 at the end of Chapter 2.

The first row in shows the regular expressions selected for classifying whether the online job posting (OJP) is explicitly open to multiple genders. These expressions are both in French and in English to reflect the languages found in the OJPs.

The second and thirds rows display job roles that were identified as potentially having (French) gendered noun endings. These selections were made by analysing a total of 628 words that appeared more than 10 times in job titles from all OJPs in 2022. The purpose was to determine which job roles were frequently mentioned in these job titles, and which of those have a feminine version of the role. This investigation means that potentially other roles (which have fewer than 10 mentions in 2022) are not included in the rest of the analysis. The comparison in the analysis in the main text pertains only to those job titles which could possess a feminised version of the role, so as to exclude roles like for example “analyste” which is both masculine and feminine and to exclude English job roles which do not have an explicit gender.

The second row pertains to words where the root of the term could encompass both the male and female versions of the job role, without also encompassing English job titles. The third row shows only the feminine versions of all most often occurring job roles. Certain roles that have the same title in French masculine version as in English, however, additionally a feminine version exists in French: assistant, agent, consultant, and expert. These words were only included in the count of potentially having a feminine ending if specific French keywords such as “sécurité” and “données” were detected, or if the female-gendered version of the role was explicitly mentioned in the job title.

The last row shows the regular expressions that are used to find female gendered noun endings. OJPs in France often mention the feminine version of a job role by adding for instance (e), (ne) or (euse) behind the male job title. A job title which contained an expression found in row four is classified as having explicitly mentioned the female version of the role in the job title.

Annex Table 3.A.1. Regular expressions for classifying cyber security jobs

<table>
<tr><th>Group</th><th>Regular expressions</th></tr>
<tr><td>Expressions for classifying job postings as explicitly open to multiple genders</td><td>"(?i)h\\/f", "(?i)f\\/h", "(?i)m\\/f", "(?i)f\\/m", "(?i)h\\.f", "(?i)f\\.h", "(?i)h \\/ f", "(?i)f \\/ h", "(?i)F ou H", "(?i)h ou f", "(?i)h\\-f", "(?i)f\\-h", "(?i)\\(hf\\)", "(?i)\\(fh\\)", "(?i)m\\/w", "(?i)w\\/m", "(?i)m \\/ w", "(?i)m \\/ f", "(?i)f \\/ m", "(?i)w \\/ m", "(?i)\\(mf\\)", "(?i)\\(fm\\)","(?i)\\(mw\\)", "(?i)\\(wm\\)", "(i?)f\\-h\\-x", "(?i)h\\-f\\-x", "all gender"</td></tr>
<tr><td>French expressions for classifying job postings as having the potential to have having gendered noun endings</td><td>"(?i)(alternant| apprenti| avocat| charg.{0,2}| correspondant| chef| chercheu| concepteu| correspondant|d.{0,2}veloppeu| enseignant|h.{0,2}berg| informaticien| ing.{0,2}nieur| intervenant| monteu| offici |technician| agente| administrateur| administratrice| animateur|animatrice|assistante| auditeur|auditrice|consultante |coordinateur| coordinatrice |directeur| directrice|.{0,2}diteur|.{0,2}ditrice| experte| formateur|formatrice| int.{0,2}grateur| int.{0,2}gratrice| organisateur| organisatrice| prÃ©sident| spÃ©cialist)</td></tr>
</table>

<table>
<tr><th>Group</th><th>Regular expressions</th></tr>
<tr><td>French expressions for classifying job postings as explicitly using the feminine word</td><td>(?i)(alternante|apprentie|avocate|charg.{0,2}e|cheffe|chercheuse|concepteuse|correspondante|d.{0,2}veloppeuse|.{0,2}ditrice|enseignante|h.{0,2}bergeuse|informaticienne|ing.{0,2}nieure| int.{0,2}gratrice|intervenante |monteuse|offici.{0,2}re|technicienne|agente| administratrice| animatrice| assistante| auditrice| consultante|coordinatrice| directrice|.{0,2}ditrice| experte| formatrice| int.{0,2}gratrice| organisatrice|prÃ©sidente| spÃ©cialiste)</td></tr>
<tr><td>French expressions for classifying job postings as including feminine endings after the male version of the role</td><td>"(?i)\\(e\\)", "(?i)\\(ne\\)", "(?i)\\((?<!v)ice\\)", "(?i)\\(trice\\)", "(?i)\\(fe\\)", "(?i)\\(euse\\)", "(?i)\\(se\\)", "(?i)\\-e\\b", "(?i)\\-ne\\b", "(?i)\\-ice\\b", "(?i)\\-trice\\b","(?i)\\-fe\\b","(?i)\\-euse\\b","(?i)\\-se\\b", "(?i)\\.e\\b", "(?i)\\.ne\\b", "(?i)\\.ice\\b","(?i)\\.trice\\b","(?i)\\.fe\\b", "(?i).euse\\b","(?i).se\\b", "(?i)\\?e\\b","(?i)\\?ne\\b", "(?i)\\?ice\\b", "(?i)\\?trice\\b", "(?i)\\?fe\\b", "\\?euse\\b", "\\?se\\b"</td></tr>
</table>

Source: OECD calculations based on Lightcast data.

Notes

[1] It's important to note that these figures are averages and actual salaries can vary widely based on factors like experience, education, certifications, and specific skills within the ICT field.

[2] Structures specialising in cyber security are primarily providers of specialised services or solutions. The professionals concerned are the first and foremost cyber security consultants; they fall within the business of consulting, service and research according to the family of ANSSI's cyber security profession overview. Specialised cyber security structures includes large consulting and IT and digital services companies, SMEs and start-ups highly specialised in cyber security.

[3] Or sometimes h/f/x to signal male/female/other gender.

[4] Given the restrictions of the French language, other genders than females are not explicitly investigated here, although job postings that for instance include words like "all genders" are also taken as explicitly being open to females.

[5] It is worth noting that the analysis is only done by investigating job titles, not full job descriptions. It is possible that certain OJPs include a gender signifier in the full text, but not in the job title. These OJPs are not counted as making use of inclusive language in this analysis. However, a job title is the first part of a job description that is read, and using inclusive language in a job title is therefore of great importance. Additionally, it is possible that certain roles with a low number of mentions in 2022 are not included in the analysis, which is discussed in Annex 1.A.

[6] However, one caveat is that it is not possible to verify whether the dataset includes the entire job title, which could mean that potentially, more OJPs originally included gender signifiers.

OECD Skills Studies

Building a Skilled Cyber Security Workforce in Europe

INSIGHTS FROM FRANCE, GERMANY AND POLAND

In an increasingly digital world, the significance of cyber security for individuals, businesses, and governments has never been greater. Rising cyber attacks are challenging current defence and operational capabilities, highlighting a critical shortage of skilled cyber security professionals. This report delves into the demand for cyber security expertise by analysing online job postings in France, Germany and Poland in between 2018 and 2023. It examines trends in the demand for cyber security professionals, the geographical distribution of job opportunities, and the changing skill requirements in this field. Focusing on France, the report also explores cyber security education and training programmes, the characteristics of the programmes, the demographics of enrolled learners, and their outcomes. Additionally, it reviews French policies and initiatives aimed at broadening the cyber security workforce and enhancing educational opportunities in this field. This comprehensive analysis is part of a larger effort to understand the evolving landscape of cyber security policies and professional experiences worldwide.

Microsoft

PRINT ISBN 978-92-64-92964-7
PDF ISBN 978-92-64-47876-3

9 789264 929647