YBER.EU.VET

Co-funded by the
Erasmus+ Programme
of the European Union

CYBER.EU.VET

KA226 – Partnerships for Digital Education Readiness

Project N. 2020-1-DE02-KA226-C31C2976

Consortium Report

on main cybersecurity challenges and best practices

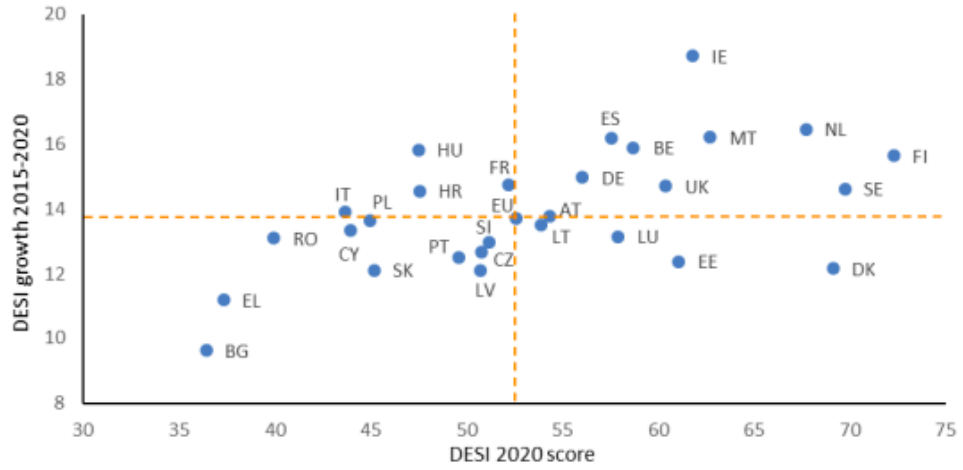
"The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Table of Contents

Introduction

Since the world is becoming increasingly digitized, it has become more apparent that practice should be combined with current policy. There is a significant focus on digital literacy policies and cybersecurity policy in the European context, however there are fewer examples of initiatives that are seen to be fulfilling these objectives in line with the policies developed. To carefully observe the extent by which digital and cybersecurity competencies are a central and divergent topic, it is useful to consider the 2020 Digital Economy and Society Index (DESI).

As part of its overall picture, DESI monitors Europe's overall digital performance and measures the level of digital competitiveness across EU countries. By providing information on the digitalization status across each Member State, it helps to identify areas for investment and further action. Towards a digital future tailored to the needs of people and respectful of EU fundamental values, the Commission presented a vision for the digital transformation "Shaping Europe's digital future" in February 2020. The DESI 2020 report assess the digital economy and society at the beginning of the pandemic using 2019 data.

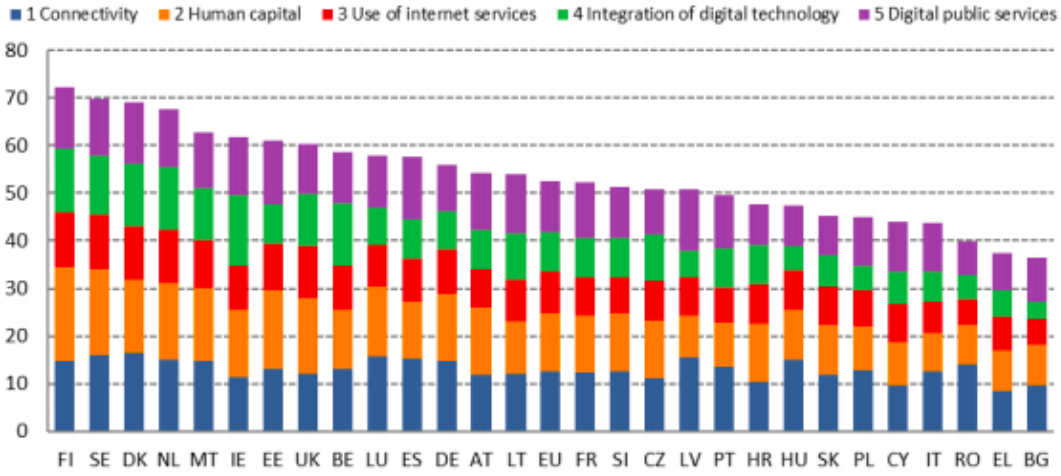


Source: DESI 2020, European Commission.

Specifically, this index investigates and gathers data about:

- Connectivity: The availability of fast and reliable internet access (including fixed and mobile connections) is vital in the current era of online delivery of key societal and economic services;
- Human capital: The backbone of the digital society is the digital skills of its people. Users of digital services and people who are limited in mobility can engage in basic activities online through these devices;
- Use of internet: As the pandemic progressed, more and more people used the Internet. Generalized confinement resulted in regular access to social media and entertainment platforms, as well as to teleworking and e-commerce services;
- Integration of digital technology: Businesses quickly adopted new working arrangements to adapt to government measures that reduced social interaction;
- In the midst of social distancing measures, it is necessary to continue governmental activities to ensure that digital public services provide benefits. It will take robust digital public services throughout the Member States to achieve a successful exit strategy from the current pandemic.

Such an analysis is helpful when considering the partner consortium which Member countries highly differentiate in terms of digital and cybersecurity performances. Indeed, three of them (in order of top-ranked, Ireland, Spain and Germany) achieve a better score than the EU- average, whereas the other four (France, Latvia, Portugal and Italy) underperform.



Source: DESI 2020, European Commission.

It is important to underline that the DESI 2020 results do not seem to confirm a linear correspondence between the country's GDP and the dissemination of digital skills. Indeed, Spain, for instance, ranked as the 5th economy of the EU only ranked as 10th on the Digital Economy and Society Index. Several initiatives have recently been introduced in some of the countries that make up the consortium to improve digitization of the economy and society. As the EU's leading country for 5G readiness, Germany has taken several measures to advance digitization, including initiatives in the areas of IT security, supercomputing, AI and blockchain. There have been numerous efforts to facilitate the digitalization of businesses and public services in France, including efforts to set up an ecosystem to support tech start-ups. The Italian government adopted 'Italia 2025' in December of 2020, a 5-year plan that places innovation and digitization at the center of a "process for radical and structural transformation of the country". In the coming years, these initiatives - which require sustained implementation over time and are also likely to require investments - might result in the progress of these member states on the DESI.

Another significant aspect when considering the level of digital and cybersecurity skills regard the impact of the COVID-19 pandemic concerning these topics. Although such a link between the health emergency and the toll of cyberattacks is not immediately clear for the most general public, in reality, the first has resulted in a increase in the latter Cybercriminals are very flexible when it comes to exploiting new events, as we have seen with the recent health emergency. With so many companies moving to new digital-first strategies in 2020 (i.e. remote working), they have inadvertently opened themselves to a range of new attack vectors that criminals have been quick to exploit. Amongst others, the COVID-19 unexpected occurrence was used to spread malware attempts: e.g., e-mails in the name of the World Health Organization, indicating that the attachment includes the latest information on the pandemic; links to charts showing the spread of the virus, the functionality of which was to steal user data; malicious emails to healthcare institutions regarding the delivery of COVID-19 protective equipment and many others.

In completing this Consortium Research Report, we utilized desk research, which consisted of locating and collecting data, publications, EU reports, national and European legislations by following references provided throughout the report. Specifically, the study explored the issue of digital literacy and cybersecurity in the different national contexts, with a focus on VET teacher training. In addition, this consortium research report highlights some of the key actors engaged in the cybersecurity sector including the national bodies and the European Union Agency for Cybersecurity (ENISA) which cooperates with Member States and EU bodies, and assists Europe in preparing towards future cyber challenges.

1.Desk research about the digital skills of VET educators

Germany:

- VET Data Report (2019) elaborated by the German Federal Institute for Vocational Education and Training (BIBB), included “digitalization” among the 3 key trends for vocational training occupations and VET in general.
- More specifically the Report stated that “Digitalization is going to reinforce structural changes of the labour market”, heading to a need for a shift in training capacities within the respective fields. As a consequence In future, the German as well as the European labour market will have particular need for more highly qualified skilled professional specialists.
- As outlined in the Resolution of the Standing Conference of the Ministers of Education and Cultural Affairs (2016-2017) – “Bildung in der digitalen Welt” (Education in the Digital World) – in the area of vocational education, the promotion of job-related competences in the context of digital work and business processes is an essential part of the teachers' competence as a starting point for their didactic activities.
- The Federal Ministry of Education and Research (BMBF) and the Federal Institute for Vocational Education and Training (BIBB) have been addressing since 2015 issues in research, development and practice, related to the digital transformation of the world of work and vocational education and training.

Ireland:

- One of Ireland’s key strategies regarding digital skills of VET educators is the National Digital Strategy which was launched in July 2013.
- The strategy focuses on digital engagement and highlights how Ireland can benefit from a digitally engaged society.

- The strategy sets out a clear vision for Ireland's digital advancement through the implementation of a number of practical actions to help increase the number of citizens and businesses engaging online through industry and enterprise, citizen training, schools and education.
- Regarding the digital skills of VET educators, evidence continues to highlight that there is an increased divide between educators who use digital devices in their class as a learning tool and those who don't.
- Many educators have stated that they feel that digital devices can 'provoke Distractions' amongst learners. However, on the contrary, many educators believe that digital devices and apps in learning activities can empower learners and support them to engage in 21st century life skills such as paying bills online/applying for jobs.

Portugal:

- The national qualifications system has reorganized VET into a single system in which programmes lead to a double certification. VET for adults is an integral part of the national qualification system, having education and training programmes for adults and recognition and validation of prior learning as key elements.
- Portugal has made significant progress regarding education attainment, but it remains lower than the EU average. Although less than 2015 (73.7%), in 2019 the share of people with low level or no qualification was 50.2%, the highest in EU.

Italy:

- In the field of education the actions were carried out mainly through the implementation of the National Digital School Plan (Piano Nazionale Scuola Digitale-PNSD).

- This is the guideline document of the Ministry of Education, University and Research for the launch of an overall innovation strategy for the Italian school and for a new positioning of its educational system in the digital age.
- Most of the actions for school staff training have been aimed at primary and secondary schools, which represent the majority of schools in Italy, while poor attention has been given to the Vocational Education and Training (VET) sector.
- In this regard, projects have been implemented for post-secondary technical education and vocational training institutes (Istituti Tecnici Superiori - ITS) with a particular focus on strengthening students' skills.
- For example, in 2019, the "ITS 4.0" project involved over 1.170 ITS students and about 130 partner companies in 106 technological innovation projects focusing on technologies such as 3D printing, virtual reality and big data.

Spain:

- The Digital Agenda for Spain (ADpE, Agenda Digital para España) published in 2013, is the road map for fulfilment of the objectives set out by the Digital Agenda for Europe in 2015 and 2020, as well as the achievement of specific objectives for the development of the economy and digital society in Spain. It is structured around six major objectives and several specific plans. The sixth objective is about promoting digital inclusion and literacy and the training of new ICT professionals. Among its specific measures, the following measures can be highlighted for the purpose of this analysis:
    - update the National Catalogue of Professional Qualifications in terms of ICT skills and training, and include this update in the training offers that accredit professional qualifications;

- maximize efficiency in the management and allocation of training funds for continuous training in ICT, both for private and public sector workers with special attention to the use of online virtual training platforms;
- assign part of the resources available for CVET to the acquisition and upgrading of digital skills of ICT professionals;
- readjust vocational training related to ICT including, among other actions specialization courses in the education remit;
- promote an improvement in the university offer aimed at training ICT professionals through their adaptation to market needs, contemplating new professional profiles in the field of ICT and increasing the efficiency of the system.

France:

- Looking at the pace of training on the use of ICT in the French universities that offer it, we can see that there are no clear and sustained policies for training trainers on the use of ICT/E. About 58% report only one training session per year compared to 7.4% per month and 0.5% per week.
- The French National Agency for the Security of Information Systems (ANSSI) has noted a very rapid increase in the level of the cyber threat in France. Continuing a trajectory initiated in 2019, the number of cyber-attacks has exploded: the number of victims has thus multiplied by 4 in one year.
- The statistics show that the density of IT training varies from one French-speaking region to another. There are several reasons for this the most significant of which are undoubtedly linked to the academic institutions and their governments.
- Further studies to see the difference could be conducted at a later stage by the regional offices or the CNFs s according to their own local or regional digital education policies.

Latvia:

- Although there is currently a lack of research studies and data in Latvia on cybersecurity and other digital skills of educators in VET and other educational institutions, it is obvious that the transition to distance learning, due to the covid-19 crises, proved to be a major challenge for many teachers.
- Regarding to national strategies, planning documents of the new budgeting period (2021-2027) highlight the following aspects:
    - The development of digital skills in the education sector (Digital Transformation Guidelines 2021-2027) – it foresees the development of digital skills of educators and heads of educational institutions, development and use of digital skills in the educational process, as well as support for the development of digital skills of employed adults;
    - The development of digital skills is included in the professional competence development programme for educators (Education Development Guidelines 2021- 2027). In 2020, the Ministry of Education and Science of the Republic of Latvia has set the improvement of educators' digital competence as a priority goal of professional competence, allocating for this purpose additional funding (0,5 million EUR);
    - The need for raising the awareness of learners and educators about information security, privacy protection and the use of reliable e-services (Cybersecurity Strategy 2019-2022, actions area "Public awareness, education and research");
    - The digital competences' development of general society (Education Development Guidelines 2021-2027, Digital Transformation Guidelines 2021-2027) as digital skills are now equated with literacy and numeracy in terms of their importance and at least at the basic level they are needed to everyone regardless the area of activity (digital skills = cross-cutting skills). The measures

should be taken to educate the population on the basic digital skills, media literacy and information literacy, which includes the whole set of basic skills, including cyber skills;

The attention that has been paid to the above-mentioned DESI index in the introduction of this research report is justified from the accuracy with which it describes the state of the art and the divergent character according to the different European countries. Such a precision is also confirmed by the single national reports concerning the digital skills of VET educators.

We believe it is particularly beneficial to compare the two extremes of the consortium, in order to understand how different degrees in digital skills affect the national population, and VET educators specifically. We will then first consider Ireland, ranked as 6th on the DESI classification.

According to the Irish Central Statistics Office (CSO), as of 2018, 89 per cent of household's have Internet access at home. Additionally, over 30 per cent of all EU data is housed in Ireland, as many of the world's largest tech companies have their headquarters located in Europe. When both statistics are coupled together, it goes without saying, ensuring that Ireland is a country that is cybersecurity ready is of crucial importance. Throughout this national report, reference will be made to the key legislation which exists in Ireland regarding both digital literacy and cybersecurity. As the world continues to adapt to 'living with COVID-19' there is a need to ensure that the anti-cybercrime landscape and best practice models continue to influence policy and practice.

One of Ireland's key strategies regarding digital skills is the National Digital Strategy which was launched in July 2013. The strategy focuses on digital engagement and highlights how Ireland

can benefit from a digitally engaged society. The strategy sets out a clear vision for Ireland's digital advancement through the implementation of a number of practical actions to help increase the number of citizens and businesses engaging online through industry and enterprise, citizen training, schools and education. In 2021, the Minister for Education Norma Foley, announced the development of a new Digital Strategy for primary level schools. The strategy is set to primarily focus on the use of digital technology in education and enhance learning through embedding technology into the future. Within the space of higher education in Ireland, one of the most notable developments is a Roadmap for Digital Learning in Higher Education: 2015 – 2017 which was developed to support a "coordinated, multilevel approach to foster digital literacy, skills and confidence among students at all levels of education".

Regarding further education and training, a relatively new Department of Further and Higher Education, Research, Innovation and Science was established. Within the departments three-year strategy, a key area of focus is regarding digital skills whereby they aim to implement a new 10-year strategy to improve literacy, numeracy and digital skills. Additionally, they focus on reforming skills training and investing in the promotion of digital skills. Regarding the digital skills of VET educators, evidence continues to highlight that there is an increased divide between educators who use digital devices in their class as a learning tool and those who don't.

Many educators have stated that they feel that digital devices can "provoke distractions" amongst learners. However, on the contrary, many educators believe that digital devices and apps in learning activities can empower learners and support them to engage in 21st century life skills such as paying bills online/applying for jobs. A final cross-government strategy which is worth noting from an Irish perspective is the 2018 Future Jobs Ireland Initiative which emphasizes a philosophy of lifelong learning. Within its five key themes, the second focuses on "innovation and technology, including preparing for the transition to the digital economy". The

strategy is central to the discussions regarding the need for further research and investment within the area of digital literacies.

Such a shared understanding and appreciation of digital means confirm Ireland as a leading country in terms of integration of digital technology. Amongst others, such an integration results as one of the main issues for the Italian context.

In Italy, less than half of the population has basic digital skills and the percentage of ICT specialists, which constitutes only the 1% of Italian graduates, is still below the EU average, although it increased in the last years. Furthermore, the data from the OECD Teaching and Learning International Survey (2013) see Italy in first place for the ICT training needs of their teachers. At least 36% of Italian teachers declared that they were not sufficiently prepared for digital teaching, compared to an OECD average of 17%, showing that specific training is needed.

In the last few years, in terms of policy response, Italy has incorporated measures on digital skills into several sectoral strategies. In the field of education, the actions were carried out mainly through the implementation of the National Digital School Plan (Piano Nazionale Scuola Digitale - PNSD), which is the guideline document of the Ministry of Education, University and Research for the launch of an overall innovation strategy for the Italian school and for a new positioning of its educational system in the digital age. It is a fundamental pillar of La Buona Scuola (law 107/2015), an operational vision that reflects the position of the Government with respect to the most important innovation challenges of the public system and, at the center of this vision, there are the innovation of the school system and the opportunities of digital education. The areas of intervention identified by the PNSD are: access, spaces and learning environments, digital administration, digital identity, student skills, entrepreneurship and labour market, digital content, staff training. Regarding this last point, the PNSD argues that teacher training must be centered on educational innovation, taking into account digital technologies as

a support for the implementation of new educational paradigms and the operational planning of activities. The objectives of this action are:

- Strengthen the preparation of the staff in the field of digital skills, reaching the whole school community;
- Promote the link between educational innovation and digital technologies;
- Develop effective, sustainable and continuous standards over time for training in educational innovation;
- Strengthen training in educational innovation at all levels (initial, incoming, in service).

In order to foster the training of teachers on IT subjects, a Memoranda of Understanding was signed with training bodies and financial resources were provided to facilitate the participation in the courses, such as:

- Memorandum of Understanding no. 785 of 22 January 2021 between the Ministry of Education and Cisco "Innovating and enhancing digital skills in the school" and "Connected and safe teachers" training program.
- Memorandum of Understanding no. 4 of 28 October 2020 between the Ministry of Education and S.O.S. The Telefono Azzurro Onlus for carrying out joint educational and training activities to promote education for digital citizenship and the conscious use of digital technologies, social media and training courses for teachers.

So far, most of the actions for school staff training have been aimed at primary and secondary schools, which represent the majority of schools in Italy, while poor attention has been given to the Vocational Education and Training (VET) sector. In this regard, projects have been implemented for post-secondary technical education and vocational training institutes (Istituti Tecnici Superiori - ITS) with a particular focus on strengthening students' skills. For example, in 2019, the "ITS 4.0" project involved over 1.170 ITS students and about 130 partner companies in

106 technological innovation projects focusing on technologies such as 3D printing, virtual reality and big data.

Another tool that will contribute to the acquisition of digital skills is included in the National Recovery and Resilience Plan (Piano Nazionale di Ripresa e Resilienza - PNRR), which is part of the Next Generation EU program, a 750 billion euro package, where nearly half of which is made up of grants, agreed by the European Union in response to the pandemic crisis. The PNRR will promote the development of digital skills of school staff to encourage an accessible, inclusive and intelligent approach to digital education. The main purpose is the creation of an ecosystem of digital skills, able to accelerate the digital transformation of the school organization and of the learning and teaching processes, in line with the European reference framework for digital skills DigComp 2.1 (for students) and DigCompEdu (for teachers). The implementation of this line of action is ensured by the Ministry of Education and will involve about 650.000 people including teachers and school staff and over 8.000 educational institutions. The government intends to strengthen vocational education, in particular the tertiary vocational training system (ITS) and STEM education, with a strong priority on gender equality.

The above-mentioned contexts represent two different national contexts. In order to have a closer indication to the general European framework, it may be useful to analyze the digital skills landscape in France, a country which on the DESI scale is very close to and immediately following the European average.

The French National Agency for the Security of Information Systems (ANSSI) has noted a very rapid increase in the level of the cyber threat in France. Continuing a trajectory initiated in 2019, the number of cyber-attacks has exploded: the number of victims has thus multiplied by 4 in one year. This is particularly worrying, especially in a context where any cyber-attack is likely to have an exacerbated impact due to the health crisis. The lack of awareness of cyber risks, the lack of control over information systems, the failure to respect computer hygiene measures, the

shortage of cybersecurity experts and, to a certain extent, the increase in the attack surface due to the widespread use of teleworking, are all weaknesses exploited by cybercriminals. The attack campaigns that hit France in 2020 successfully disrupted many businesses and caused significant financial losses. The massive use of outsourced digital services, often less secure, is a widespread practice that attackers do not fail to exploit. The statistics show that the density of IT training varies from one French-speaking region to another. There are several reasons for this. Among them, the most significant is undoubtedly related to academic institutions and their governments. Further studies to see the difference could be conducted at a later stage by the regional offices or the CNFs according to their own local or regional digital education policies. The training statistics show that the thematic needs that have been the subject of training workshops also vary from one region to another. The thematic frequency in this sense also depends on endogenous factors related to demand and supply according to the needs and levels of advancement in the fields of ICT/E and ODL of local partners.

2.Desk research about the main digital security issues in partner countries

Germany:

- To analyze the specific German context and draw a needs analysis, is especially significant the review of the 2020 Digital Barometer, a representative online survey of private citizens on cybersecurity, conducted jointly by the BSI and the German State and Federal Police Crime Prevention Commission.
- In recent years, within the German and European landscape, cybercrime has been the major cause of recent cyberattacks. The 2020 BSI report confirmed data leaks and critical vulnerabilities found in software and hardware products. This research has also noticed a rise in mass cybercrimes targeting private citizens, commercial enterprises, and other institutions using malware.
- The most common vulnerability exploited by malware is a vulnerability in the host system. In the case of software or hardware products, vulnerabilities can be found in gateways, such as those that operate between offices or production networks, or they can be caused by human error in social engineering.
- This degree of digitalization is not without its risks and dangers. One in four respondents reported they had been a victim of cybercrime in the past year. The overall rate of cybercrime in 2020 remains constant. Online shopping and third-party access to online accounts are the most common types of fraud that affect victims (44%) and (30%), respectively.

In spite of the findings, two-thirds of respondents expressed a desire for more information about preventing data theft (66%). Advice sought most often consists of practical tips such as

ways to ensure secure passwords for multiple online accounts (59%), followed by advice about which software is best-suited to protect online accounts (52%), and advice about the pros and cons of password managers (49%).

Ireland:

- Cybersecurity threats in Ireland are continuing to rise, with the most recent cybersecurity attack taking place in 2021 on Ireland Health Service Executive (HSE) which has and continues to have devastating effects on Ireland's health care system.
- Ireland is home to over 30% of the EU's data due to the number of Cybersecurity Centers with their headquarters in the country. Although this provides many opportunities, it also results in increased level of threat of cybercrime. As Ireland is an open liberal democracy, it is seen as being particularly vulnerable to so-called "hack and leak" type attacks.
- Ireland's second National Cybersecurity Strategy 2019 – 2024 was launched in a bid to increase the cybersecurity readiness of the country. The key objectives of the strategy are:
    - To ensure Ireland's cybersecurity readiness and respond to, and manage cybersecurity incidents, including those concerning national security,
    - To protect and manage any disruption of services involving critical national infrastructure from cyberattacks,
    - To further grow and develop the cybersecurity sector in Ireland and be cyber-ready,
    - To implement the best technology and measures available internationally in Irish businesses,
    - To increase awareness and develop skill sets among organizations and private individuals around cybersecurity.

- In 2018, an Action Plan for Online Safety was launched and contains twenty-five actions under five main goals centered around legislating criminal offences regarding cybercrime, removing illegal and harmful material and prompting online safety.

Portugal:

- The main digital security topics to assure are:
    - Foundation level
        - Identify the exposure of your school infrastructure and applications in the online environment and adopt risk mitigation measures (both structural and behavioral);
        - Identify and mitigate vulnerabilities;
        - Identify personal information on internet that can be used on a attack;
        - Acquire a set of appropriate behaviors in the use of cyberspace;

    - Intermediate and Advanced levels:
        - Security Programming Technical Environments
        - Social engineering
        - Exploring Open Data Sources
        - Wireless Networks
        - Encryption and Passwords

Italy:

- The most widespread security problem in the last three years in Italy is password phishing, indicated by 48% of Italian managers, against 36% of European managers. Moreover, 28% of Italian managers have problems related to access and identity (in line

with the European percentage) followed by the problem of social engineering-based malware (24%).

- Furthermore, only 42% of people between 16-74 years old have basic digital skills and the percentage of graduates in IT and ICT subjects is very low compared to European data.
- Government tackles digital skills in “Italia 2025”, a five-year strategy for innovation and digitization launched in 2019. In particular, the strategy includes “Digital Republic”, an initiative promoted and coordinated by the Ministry for Technological Innovation and Digitization.
- The initiative aims to build an alliance between public and private organizations and citizens, and invite them to take concrete action to promote digital skills. It focuses on three lines of action:
    - boosting basic digital skills;
    - promoting upskilling and reskilling of the workforce;
    - developing ICT and emerging technologies skills.
- A further step forward will be taken with "Italia digitale 2026" which sets five ambitious goals to be achieved in the coming years:
    - Disseminate digital identity, ensuring that it is used by 70% of the population;
    - Bridging the digital skills gap, with at least 70% of the population being digitally capable;
    - Bring about 75% of Italian PAs to use cloud services;
    - Reach at least 80% of essential public services provided online;
    - Reach, in collaboration with the Mise, 100% of Italian families and businesses with ultrabroadband networks.

Spain:

- Spanish Activation Strategy for Employment 2017-20 aims to consolidate the economic recovery by promoting Cybersecurity Programmes and Resources for VET Institutions to meet the challenges of the present and future labor market deriving from globalization and digitalization. It establishes the measures to be carried out, at both the state and regional level, by the Public Employment Services (PESs);
- In quantitative terms, one of the objectives is the training in digital skills of at least 225.000 young people: 75% in basic skills and 25% in advanced digital skills, which represents 40% and 38% respectively of the young population under 30 years.
    - start-up support to technology-based projects for young women, providing a consultant to advise these entrepreneurs about their business plan and offering monitoring services;
    - specific training actions for young women from rural areas in ICT technologies and new future sectors, taking advantage of the possibilities of new technologies and with trainers and tutors, including online teaching;
    - promotion of entrepreneurship, self-employment and new job opportunities offered by the digital economy and the different formulas of the social economy and the economy of digital platforms, within employment activation policies;
    - improving the visibility of best practices developed to understand what are the main digital security topics.
- National Operational Programme on Youth Employment (budget 39 million Euros). As an example, the Programme includes a Training pathway on Digital Transformation for employment.
- The Project, implemented by EOI with the partnership of Google, is aimed at improving the employability of young people who have dropped out of school from an early age, have lost their jobs or have difficulties finding their first job.

France:

- The ministers of higher education of the French-speaking world met on 5 June 2015 in Paris at the joint initiative of France, the OIF (Organisation internationale de la francophonie) and the AUF (Agence universitaire de la francophonie) to examine the state of and prospects for the digital development of the French-speaking university & VET space.
- The main aim of this work was to contribute to the elaboration of a Francophone strategy for the training of trainers in the field of digital education and to assess the training needs and expectations of the target groups concerned, and then to determine what is needed to meet these needs and expectations, notably in terms of services, content and competences.
- According to the study "Étude sur l'identification des besoins en formation tic/e dans les pays francophones du sud, 2016", The needs of teacher-researchers are strongly marked by a unanimous trend towards training in ICT/E and capacity building related to digital education (80.4%).
- The digital risks are very present in the representations of young teachers, who easily relay the media discourse. The three risks that teachers feel they face most personally are technical (66.20%), ethical and legal (55.80%), and informational (54.70%).

Latvia:

- According to the national Cybersecurity Strategy 2019-202215, Latvia's cyberspace continues to face large-scale threats – phishing, extortion and malware, attempts to hack the systems, networks and websites, denial-of-service attacks (DoS) on critical

information systems as well as fraudulent e-mail and social engineering campaigns to retrieve personal or authentication data to discredit a specific person, company or institution or to commit crimes.

- Both in Europe and in Latvia, the following incidents became topical – money extortion attempts primarily aimed at financial institutions or private sector companies (attackers performed a series of trial attacks, threatening to suspend the operation of company websites or other resources by means of attacks of up to 2 Tb/s).
- At the of 2021, fraud, malware and vulnerabilities continue to be active - stolen WhatsApp accounts through activation codes which requested by hacked accounts of person's contact list; a new wave of blackmail emails (sextortion) – threaten to distribute compromising material, if e-mail user will not make a ransom.
- The year 2020 with its global changes have demonstrated that for educators of the VET and other education institutions it is important to have increased knowledge/skills on the safe remote work when organizing online classes and using digital tools (e-mails, WhatsApp, learning platform, etc.) as well as to be aware about the topical scams and frauds, especially on social media, to raise the awareness of their pupils and students.

Although the link between the COVID-19 pandemic and the toll of cyberattacks is not immediately clear for the most general public, in reality, the first has resulted in an increase in the second. Cybercriminals are very flexible when it comes to exploiting new events, as we have seen with the recent health emergency. With so many companies moving to new digital-first strategies this year (i.e. remote working), they have inadvertently opened themselves to a range of new attack vectors that criminals have been quick to exploit.

The national offices offer a multifaceted perspective on the main digital and cybersecurity issues. As distance learning becomes the new normal, cybercriminals are finding new ways to leverage techniques such as phishing, ransomware, social engineering, and more to launch their attacks. Here are some of the most critical risks encountered.

1. Secure remote access

As distance learning takes over from physical teaching, students and teachers need access to online learning tools mainly located in the cloud, i.e. file-sharing applications, emails, applications, and they sometimes need to access resources on the school network remotely. If remote access is not secured, hackers can penetrate the system and take control of the entire network.

2. Access to sensitive data

Educational institutions contain a treasure trove of sensitive data that can be sold on the dark web. The personal data of students, teachers, alumni and administrative staff, as well as sensitive data relating to a school's research and intellectual property, can be a real treasure trove for a hacker to sell or ransom. It is therefore essential to implement identity-based access, allowing authorized users to access only the resources they need to do their job.

3. Malware

The move to distance learning means that many devices connected to the school network are BYOD (Bring Your Own Device). It is difficult to know whether the devices and applications used are properly updated with patches and whether the antivirus itself is up to date. Unless these remote devices connect via a VPN, you need to ensure that they are secure before they can access resources on the training network. It is important to deploy advanced web protection capabilities that can identify and block the latest web threats.

4. Phishing

Social engineering and phishing attacks are major cybersecurity risks for French training centers. Trainers and teachers or staff members who are tricked into clicking on malicious links can give cybercriminals access to the school's network and valuable resources. The best way to counteract social engineering and phishing attacks is through user awareness and training. Training and testing your users with simulated attacks will help build a positive culture of security awareness and make them less vulnerable to various online scams.

5. Fraud

Regarding fraud, the year 2020 was reported to be very intensive, including social engineering attacks. Among the most active fraud attempts were extortion campaigns, where hackers claimed to have hacked a user's device and obtained compromising material for which a ransom was set; fraudulent lotteries on behalf of the known brands, offering to win the newest smartphones or other valuable prices.

A new trend was observed - extortion e-mails with the threat of leaking data. On many occasions, companies were targeted. Misleading advertisements on social media – using the names of famous people without their knowledge, invited internet users to invest in cryptocurrency. Scammers also made phone calls and tried to persuade people to invest. In certain cases, repeated fraudulent attempts were observed where the victims of financial fraud were offered help to get their lost resources back.

Phone scams – by falsifying the phone numbers of different credit institutions and pretending to be bank representatives, scammers, using the public's poor knowledge on additional authentication methods, defrauded financial resources from several thousand users, causing total losses worth hundreds of thousands to Latvian credit institutions. Hackers' adaptation to the necessity to start remote work – considering the needs of companies to rapidly switch to a remote work condition and implementation of electronic documents' circulation, hackers used

the situation to ad e.g. a number of company accountants received emails in the name of the director or another employee to make an urgent payment or change the payroll account.

Interference in business correspondence of companies – by compromising the emails of companies or their collaboration partners, allowed for attackers to pick a suitable moment to send one of the parties a bill with a changed account.

Many internet users were target of scam messages with shortcut links (ej.uz), used to mask the actual link destination, on behalf of the state institutions regarding the state of emergency and the epidemiological situation in the country.

Fake online stores – specifically high activity have been observed during the holiday season by means of social media advertisements and due to the covid-19 restrictions which forced companies to sell their products online.

It can be useful to employ some data reported by the national reports. For instance, in France the digital risks are very present in the representations of young teachers, who easily relay the media discourse. The three risks that teachers feel they face most personally are technical (66.20%), ethical and legal (55.80%), and informational (54.70%). Psycho-social, cognitive and socio-economic risks seem to worry them less. There is a systematic discrepancy between the representations of risks for themselves compared to those for the pupils. Indeed, the three risks that teachers feel their pupils face most are psycho-social (69.95%), informational (70.75%) and technical (62.80%). Teachers therefore feel the same vulnerability as their students with regard to technical risks, but consider their students to be more exposed to problems relating to harassment or false information in particular. The amplification of risks for students can be explained by the fact that teachers perceive them as being very vulnerable. A trainee teacher described her fourth-grade pupils as very vulnerable, quite naive, not necessarily aware of the potential danger of the networks.

Germany's Federal Office for Information Security (BSI) report noted that several campaigns exploited the confusion and fear created by COVID-19, including malware and phishing campaigns, CEO fraud, and scams. Additionally, the BSI said such events might have increased the chances of success for such attacks because of the fears, worries, and insecurities associated with such events. In recent years, within the German and European landscape, cybercrime has been the major cause of recent cyberattacks. To analyze the specific German context and draw a needs analysis, is especially significant the review of the 2020 Digital Barometer, a representative online survey of private citizens on cybersecurity, conducted jointly by the BSI and the German State and Federal Police Crime Prevention Commission. The digital transition is actively shaping our everyday lives from online shopping to wearables (such as fitness-tracking armbands, smartwatches or smart glasses), new payment and ID schemes.

However, this degree of digitalization is not without its risks and dangers. One in four respondents reported they had been a victim of cybercrime in the past year. The overall rate of cybercrime in 2020 remains constant. Online shopping and third-party access to online accounts are the most common types of fraud that affect victims (44%) and (30%), respectively. Most respondents in the survey were familiar with the recent cybersecurity recommendations on preventing cybercrime. These recommendations are generally followed only when it makes sense for the person to do so (41%) or who has just learned about a particular piece of advice (39%). Research shows that people who have already been victims multiple times are more likely to heed advice only when a problem arises (33%), even if they were already aware of it. Eventually, in spite of the findings, two-thirds of respondents expressed a desire for more information about preventing data theft (66%). Advice sought most often consists of practical tips such as ways to ensure secure passwords for multiple online accounts (59%), followed by advice about which software is best-suited to protect online accounts (52%), and advice about the pros and cons of password managers (49%).

Eventually, another significant perspective is offered by Ireland and the cybersecurity threats occurred in 2021. A massive and coordinated attack started in May 2021, disrupted the health service and computer systems across the country, stole personal data of a high percentage of patients and continues to demand a ransom for the return of data. In response, the Health Service Executive (HSE) has had to shut down hospital and health service IT systems to protect against any further data being stolen. Many services have been disrupted and personal and medical information leaked. However, it should be noted that there is no evidence to support the acquisition that further scams involving people's information has taken place. Ireland is home to over 30% of the EU's data due to the number of Cybersecurity Centers with their headquarters in the country. Although this provides many opportunities, it also results in an increased level of threat of cybercrime. As Ireland is an open liberal democracy, it is seen as being particularly vulnerable to so-called "hack and leak" type attacks. Generally, these attacks are seen to be politically motivated and are centered around misinformation and "fake news" used as an attempt to destabilize the State.

Many involved in the sector of cybersecurity are calling for increased investment in government bodies such as the National Cyber Security Centre (NCSC) in Ireland. Other threats/risks which continue to prevail themselves are the risks posed to Critical National Infrastructure (CNI), public sector systems and data which has been outlined briefly in previous paragraphs. New issues which begin to emerge are those connected to the deployment of 5G technologies. Although this will give rise to new technologies and services, cybersecurity needs to be at the forefront of thinking as many countries begin to adapt.

Outside of a national and business perspective, cybersecurity crimes continue to occur prolifically on a daily basis amongst the average person. They are often not reported to law enforcement with only five percent of cybercrimes allegedly reported to the police in Ireland in 2019. Furthermore, a 2019 report commissioned by Microsoft in Ireland finds that employees are still seen to be the 'weak link' in the security system due to lack of security training, poor

password management, the use of personal devices with work-related data and potential violations of the EU General Data Protection Regulation.

3.Best practices of Cybersecurity Programmes and Resources for VET Institutions in European Union and in each partner Country

As specified in the introduction the Cyber.EU.VET Project involves a multifaceted and diverse consortium. Concerning digital and cybersecurity skills, the consortium partner countries perform to different degrees of effectiveness, as perfectly described by the DESI index.

Academic analysis and evaluation of good practices was an integral part of the research work carried out at national level by each partner in the project consortium. This research had as a common guideline a need analysis of VET issues at local and national level. In carrying out this work, the seven national partners shared some difficulties related to the search for training initiatives and cybersecurity specifically designed for VET teachers. While this has made this task rather difficult, it has also shown even more clearly the importance and need to develop projects in this area. It then confirmed the extremely innovative spirit of the CYBER.EU.VET project. Here is a collection of the most relevant good practices found by each partner.

3.1 Germany - VET 4.0 Initiative

VET 4.0 is an umbrella initiative, collaboratively developed by the Federal Ministry of Education and Research (BMBF) and the Federal Institute for Vocational Education and Training (BIBB) from 2016, that brought together a wide range of projects within three main pillars. Pillar 2 of this comprehensive initiative (which is still ongoing) is completely dedicated to “digital literacy/media competence”, and aims to define media competences, which should be considered as an entry requirement and as a key competence across occupations in VET (for apprentices, teachers and trainers). Funding programmes to better equip training centers and to support small and medium enterprises (SMEs) in view of digitalization complement this

approach of promoting media competence in VET. Through the special ÜBS digitisation programme (71), the BMBF and BIBB are helping to accelerate the digitalization of processes in the training of apprentices in the context of 'VET 4.0'. The special programme consists of two lines of funding:

1) Funding is provided to purchase selected digital equipment (digital devices, machines, systems and software, such as smart home technologies, 21 industrial robots, 3D printers and digital teaching and learning media, such as tablets and touchscreens), in order to modernize the training of apprentices, especially for those trained by SMEs;
2) The programme also funds 8 pilot projects in competence centres that identify the impacts of digitalization on the vocational activity profiles and determine requirements and consequences resulting from this for the qualification of skilled staff and training personnel. In a second step, they develop innovative teaching and learning concepts for VET 4.0 and disseminate them as multipliers. The aim is to ensure that outcomes are transferable, and that there is a broad range of applications.

The following are some examples of the aforementioned pilot projects:

- "Digital Media in VET" that will end in 2022 and which is composed by several sub-programmes with different funding priorities are funding national digital training projects that develop new learning scenarios and modern initial and continuing training courses promoting the acquisition of digital media competence;
- "Qualification Initiative Digital Change - Q 4.0", which, from 2018, has been funding the development and testing of further training concepts for in-company VET trainers. The project consists of two sub-projects: 1) MIKA seminars (Media and IT Competence for Training Personnel) to promote basic media pedagogical competence, the development and testing of continuing education modules to strengthen the basic media and IT skills of training personnel; 2) Q 4.0 NETWORK aiming at adapting training process to digital

change, also taking into account regional and sector-specific differences. In both projects, the end result could be a prototype of a tested seminar offer that could be made available to VET staff nationwide;

- "Digitalization II" since 2018 to identify strategies for designing learning processes that use the potential of digital media to support successful learning, both for individuals and groups.

3.2 France - Internet Sans Crainte

(Since there is a lack of VET field good practices within this specific country, this case study has been selected as a practice that fulfills the required constraints but does not specifically concern the VET sector).

In view of the constant cases of cyberbullying, Internet addiction, dangerous encounters on the web, and their tragic consequences for very young students, it has become necessary to draw everyone's attention to the rights and limits of online behavior and, above all, to present the Internet as a tool for enrichment and entertainment free from danger. Created in 2000, pioneer in digital pedagogy and expert in young public communication, Tralalere is a leading producer of cross-media educational programs: cartoons for multimedia productions, serious games, mobile apps, eBooks etc. Notably, Tralalere conceived and directed the national program raising awareness to risks on the Internet: www.internetsanscrainte.fr.

Operated by Tralalere since 2008, Internet Sans Crainte is the national programme to help young people gain better control over their digital lives. In concrete terms, Internet Sans Crainte offer a hundred or so free turnkey resources to help teachers, educators and parents to support

young people aged 6 to 18 in their to help teachers, ducators and parents guide young people aged 6 to 18 towards an enlightened and responsible use of screens and digital technology. Internet Sans Crainte also offer advice and expertise on how to support young people in their digital education through thematic files. Tralalere and Internet Sans Crainte also coordinate Safer Internet France, national and European programme for the protection of minors on the Internet, alongside the Net Ecoute (e15 Enfance) line and Point de contact. In this capacity, Internet Sans Crainte organizes Safer Internet Day in France, a worldwide day to raise awareness among young people to better use the Internet. This programme is supported by the European Commission as part of the Inhope/Insafe network, which includes 38 countries.

BENEFICIARIES

Internet Sans Crainte, offers all year long digital resources adapted to different audiences, including:

- Educational mediators (teachers, animators, librarians, etc.);
- Parents and families;
- Institutions and associations.

3.3 Ireland - Cybersafe Kids

(Since a lack of VET field good practices exist within this specific country, a practice has been selected that fulfill the required constraints but does not specifically concern the VET sector).

Cybersafe Kids as a project began in 2015 and has now become a recognized charity funded by a number of Irish Philanthropic Funds such as The Ireland Funds. Cybersafe Kids delivers a number of training programmes focused on cybersecurity in schools across the country of Ireland. Cybersafe Kids' vision is for a world in which children are using technology in a safe, positive and

successful manner. The primary stakeholders of Cybersafe Kids are participating schools across Ireland (the students, teachers, principals and guardians), partnering research universities, the funders of the charity and the team involved in the delivery of the programmes. The charity's main objective is to advance, promote and provide education and training to children, parents and teachers in the community to ensure safe and responsible navigation of the online world. Regarding impact, to date, Cybersafe Kids has reached 24,000 children between the ages of 8 and 13 via their schools programmes. In 2020 alone, the programmes liaised with 5,986 children and 1,554 parents in 56 schools in Ireland. Additionally, an anonymous online survey was distributed which gathered data from 3,764 children aged 8 – 12 regarding their online use. According to the Directors Report (2019) the primary areas of impact included the following:

- The delivery of an Education Programme and the launching of a behavior change measurement project in partnership with the University of Dublin and the Children and Young Persons Committee (CYPSC);
- Hosting of a strong 'Safe Internet Day' campaign;
- Launching online content and resources targeting parents of younger children (Aged 2-10). In previous years' material was published for older children;
- Development of a series of policy 'asks' which aim to impact overarching country policy regarding cybersecurity.

3.4 Spain – SPACE: Skills for school professionals against cyberbullying events

BACKGROUND.

The widespread diffusion and use of new technologies is connected to the phenomenon of cyberbullying. In 2009 across Europe approximately 18% of European young people aged 13-19 had been bullied/harassed/stalked via the internet and mobile phones, current rates ranged

from 10% to 52%. European Parliament highlights that cyberbullying increased among children aged 11-16 from 7% in 2010 to 12% in 2014.

NEEDS OF THE TARGET GROUPS.

The project SPACE answers to the training needs of school teachers, in order to make them acquire competences to prevent/contrast cyberbullying. In fact, despite the EU Member States launching many initiatives and projects to prevent and combat cyberbullying, it appears to be growing: since it is a new phenomenon, it lacks an organic system of knowledge, skills and structured educational actions ensuring that teachers acquire the knowledge of its dynamics, the mastering of the digital technologies for a safe use of the Web, and the competences to plan action of prevention, information and training.

OBJECTIVES.

Many resources and contents about cyberbullying have been developed by schools and institutions; nevertheless, they were isolated initiatives, not collected into a single web space and thus were not valorized. SPACE has taken up this challenge and has developed a MOOC - free online open course - on cyberbullying for school teachers, and a multilingual Public Digital Library of Open Education Resources on cyberbullying. Project main purposes:

- to map and describe the competences needed to prevent and contrast cyberbullying;
- to develop a digital library of OER on cyberbullying, with advanced search features;
- to develop a MOOC for school teachers on cyberbullying, using the previously retrieved and labelled OER;
- to potentiate and improve in the involved teachers the digital competence, namely cybersecurity, web risk and net etiquette;
- supporting teachers acquiring the competences to intervene in case of cyberbullying at school and to plan and realize information and training activities with their students.

PARTICIPANTS.

The main target group involved in the project is represented by school teachers (ISCED2 and ISCED3 levels). Indirect target groups were school manager and nonteaching staff; students; parents; school authorities and decision makers. 139 teachers were involved in the MOOC trial and 300 participated in the Multiplier events organized in the partner countries. The Public Digital Library received over 8.000 visits during the project's lifecycle.

ACTIVITIES.

The project lasted 24 months, during which the following activities took place:

- realization of a map of competences and a MOOC model;
- design and development of an online digital library on cyberbullying;
- retrieval, cataloguing and identification of OER on cyberbullying, and implementation of these resources in the digital library;
- setting up and customizing a CMS platform to host the MOOC;
- design, development and testing of a multilingual MOOC on cyberbullying;
- creation of a Toolkit with indications, guidelines and recommendations on the SPACE system and tools;
- realization of 10 Multiplier Events in the partner countries and a final conference;
- realization of 4 consortium meetings;
- dissemination through the creation of a website, brochures, presentations, participation as a reporter invited to the DIDACTA Fair in Florence, articles in magazines and newspapers.

IMPACT.

The project has produced a positive impact, promoting awareness of cyberbullying, greater knowledge of its dynamics and methods of prevention and contrast, and developing a multidimensional set of knowledge and skills in the group of European teachers involved.

Teachers and organizations involved in the testing have acquired competences in order to prevent and contrast cyberbullying, specialist digital competences on cybersecurity, web risks and net etiquette, developed strategic skills and methodological-didactic competences improving their teaching professional, have available more effective instruments in order to carry out information and training activities for their students to prevent cyberbullying.

3.5 Latvia - Programme "Improvement of Teachers' Digital Competence in the Form of E-Environment for the Use of Educational Technologies"

OBJECTIVE.

The aim of the Programme is to improve educators' digital competence – to teach about technologies and tools that will help educators to organize their work process more efficiently. Programme is implemented by since 2014 by the Ministry of Education and Science of the Republic of Latvia.

BENEFICIARIES.

The content of the courses in 2020 is designed for:

- management teams of educational institutions;
- educators of vocational (VET) and general education schools;
- primary school teachers;
- pre-school teachers;
- various subjects' teachers (math, Latvian language, computers science, engineering, design and technology, physics, chemistry and biology).

DESCRIPTION.

In 2020, the Ministry of Education and Science has set the improvement of educators' digital competence as a priority goal of professional competence, allocating additional funding. The programme offers free-of-charge course for educators with different knowledge level representing various subjects (their field of specialization, see section Beneficiaries). The implementers of the courses have developed detailed learning tasks, attracted group leaders - consultants to ensure a favorable learning regime for educators. The content of the courses is designed in accordance with the requirements of the modern learning environment.

RESULTS ACHIEVED.

4339 educators have attended long (with the granted right to work as computer science teacher)

and short professional competence development courses (2014-2020).

INNOVATION.

Innovative approach hinders in the process organization – each course participant can learn the content at a pace and time convenient for them. During the course, technologies and tools are analyzed that can be used in the study process in order to promote collaboration and simplify the organization of the study process/educators' work process.

3.6 Portugal

Despite some ad-hoc initiatives, training actions in the area of cybersecurity for VET were not identified. Only several higher education courses, postgraduates or of a business nature were identified in the market, so cybersecurity training for VET should be a fundamental priority to underpin the more cybersafe future of our country, namely capable of guaranteeing personal and business security.

The National Cybersecurity Centre, with the mission of promoting the sharing of knowledge and a national Cybersecurity culture, developed the Awareness and Training Program in Cybersecurity, through which it is intended to massify the training and awareness of citizens and employees of organizations for the dangers of the uninformed use of cyberspace, by carrying out actions to raise awareness and training in Cybersecurity in different parts of the country, from north to south, passing through the islands, with the support of partners, but nothing directed to VET Institutions.

3.7 Italy - Docenti connessi e sicuri (Connected and safe teachers)

BACKGROUND.

The programme has the general objective of carrying out actions aimed at innovating and strengthening digital skills in schools. Specifically, the programme aims to improve the skills and knowledge of teachers regarding new integrated digital teaching experiences, the functioning and benefits of the Internet of Things and the importance of cybersecurity. The programme is promoted under the new memorandum of understanding between the Ministry of Education (Italy) and Cisco.

TARGET GROUPS.

The beneficiaries of the program are teachers of Italian schools of any order and grade.

ACTIVITIES.

The training programme offered by Cisco to teachers consists of 3 webinars to which 3 in-depth courses are linked. Participation in the entire program is totally free.

1. A connected digital world Webinar “DAD and new experiences of integrated digital teaching” held by Cisco personnel or Cisco Partners and linked online course “Get

Connected". Estimated time to complete: 30 hours Course Overview: The course teaches you to develop basic digital knowledge. The particularly interactive course structure creates an easily accessible environment for an audience approaching the world of IT for the first time.

2. Conscious digital citizens: Webinar "Smart City and Internet of Things: new digital services for citizens" held by Cisco personnel or Cisco Partners and linked online course "Introduction to the Internet of Things (IoT)". Estimated time to complete: 20 hours Course overview: The Introduction to the IoT (Internet of Things) course introduces teachers to the technologies that support the IoT and the opportunities generated by the growing number of network connections between people, processes, data and things.
3. IT security: Webinar "How to protect yourself from network threats" held by Cisco personnel or Cisco Partners and linked online course "Introduction to Cybersecurity". Estimated time to complete: 20 hours. Course overview: The Introduction to Cybersecurity course analyzes trends in the IT world, threats and the fact of being in total security in cyberspace, protecting personal data.

IMPACT.

Since the project ended on June 3, the numbers concerning the teachers trained are still being elaborated. However, the project is innovative because it combines technology-related training with digital entrepreneurship, but also with programming.

Conclusion

The research conducted for the project CYBER.EU.VET revealed that there is a lack of data and information on the cybersecurity competences and challenges of educators of education institutions at the European level, as well as that there is a limited number of initiatives focusing on the cybersecurity issues within the VET, indicating that project CYBER.EU.VET have addressed the emerging topic across the Member States.

Nevertheless, those existing initiatives are comprehensive and proved to be efficient (see section Good Practices). Currently, most of the activities and projects are focusing on the cybersecurity awareness raising of general population and improvement of overall digital competencies of educators, which was influenced by the rapid adaptation to remote work/learning process.

The partner consortium is multifaceted and a clear expression of a different extent of digital skills throughout Europe. However, regardless of the DESI ranking of the individual countries, this Consortium Research Report can be used to draw meaningful and valid indications for the entire European context.

The feeling of a need for training is clear, even among those VET teachers who have already been trained in ICT. There is no rejection of the need for training, nor any questioning of its usefulness. We also note that the more teachers feel exposed to psycho-social, ethical, legal, technical or health risks, the more they say they feel a need for training.

According to a national survey, more than half of teachers who feel vulnerable to cyberbullying feel that training is needed. For them, initial and continuing education is an opportunity to share

experiences and analyze methods of professional practice in this field. It is still believed that using digital tools in education is a way to teach or an object to be taught to students rather than an integral part of their general culture.

A culture of information sources and practices on digital risks (research and monitoring) should be developed. Training must also be stepped up on the challenges of digital technology and in particular on the psycho-social, ethical, legal and technical problems that can arise in the use of digital tools and which worry teachers to the point of leading them to give up all use.

Thus, knowledge of digital risks can positively influence pedagogical practices for educating students in digital literacy. A teacher with a strong digital culture will be more inclined to use digital technology in the classroom with his or her pupils and to make digital technology a teaching-learning object.

The obvious influence of the representation of risks is impossible to change positively without a general and plural digital culture, complementary to an information culture in the broadest sense, which avoids demonizing the technical object and enables the educational potential to be exploited. It is not a question of educating in fear, but of emancipating (and being emancipated, as a teacher too) through a critical and enlightened apprehension of the digital world.

References

ADEI (2017), *El trabajo del futuro*. Technical Note.

Agence nationale de la sécurité des systèmes d'information (ssi.gouv.fr)

Andries B. et Beigbeder I. (coordonné par) (1993), *La culture scientifique et technique pour les professeurs des écoles*, Paris: Hachette éducation, CNDP.

Baron G.-L. et Baudé J. (1992), *L'intégration de l'informatique dans l'enseignement et la formation des enseignants*, Tours: EPI - INRP.

Baron G.-L. et Bruillard É. (2000), *Technologies de l'information et de la communication dans l'éducation : Quelles compétences pour les enseignants?,* Éducation et Formation, No 56.

Baron G.-L. et Bruillard É. (sous la direction) (2002), *Les technologies en éducation: perspectives de recherche et questions vives*, Actes du Symposium international francophone, Paris : INRP, IUFM de Basse-Normandie, MSH.

BIBB (2016), *"Economy 4.0 needs Education 4.0", Strengthening the media competence of training staff and trainees*

Blanco, R., Fontrodona, J., Poveda, C. (2017), *La industria 4.0: el estado de la cuestión,* Revista Economía Industrial, No 406.

Buisán García,M.; Valdés, F. (2017), *La industria Conectada 4.0.*, Revista de economía, No 898.

Bihouix P, Mauvilly, K (2016), *Le Désastre de l'école numérique*, Le Seuil.

Capelle, C., Cordier, A., Lehmans, A., (2018), *Usages numériques en éducation : l'influence de la perception des risques par les enseignants*, Open Edition Journals.

Carrizosa Prieto, E (2018), *Lifelong learning e industria 4.0. Elementos y requisitos para optimizar el aprendizaje en red.*, Revista internacional y comparada de relaciones laborales y derecho del empleo. Vol. 6, No 1.

Central Statistics Office (CSO) (2018), Information Society Statistics – Households: https://www.cso.ie/en/releasesandpublicatons/er/isshh/informationsocietystatisticshouseholds2018/ (accessed on 6th July, 2021).

CEFEDOP, (2021), *Vocational education and training in Portugal*, EU Agenda.

Cyber Ireland, (2021), Cyber Security Skills Report 2021: National Survey: https://www.cyberireland.ie/wp-content/uploads/2021/02/Cyber-Ireland-Skills-Report2021.pdf(accessed on 3rd July, 2021).

Database of National Education Opportunities – Niid.lv, study programmes in cybersecurity

Department of Education and Skills, Government of Ireland (2015), *Digital Strategy for Schools (2015-2020)-Enhancing Teaching, Learning and Assessment.*

Department of Education and Skills, Government of Ireland (2017), *Higher Education System Performance Framework 2018-2020.*

Department of Enterprise, Trade and Employment (2018), *Future Jobs Ireland – Preparing Now for Tomorrow's Economy.*

Department of Further and Higher Education, Research, Innovation and Science, Government of Ireland (2021), *Statement of Strategy 2021-2023.*

Department of Justice (2021). Cybercrime: www.justice.ie/en/jelr/pages/cybercrime (accessed on 2nd July, 2021).

Department of Tourism, Culture, Arts, Gaeltach, Sport and Media (2019), *Action Plan for Online Safety 2018 – 2019.*

Dig8tal (2020), *Is German Cybersecurity ready for 2021?,* https://dig8ital.com/resources/library/is-german-cyber-security-ready-for-2021

Erasmus+ project DIG4VET (Digital Tools for Learning and Validation in VET and WBL: Training Program
for VET Teachers, Trainers and Potential I-Coaches)

Escuela de organizacion industrial, *Activa industria 4.0.*

EFVET (2021), *Digital Balance: Balancing Digital Competences and Wellbeing.*

European Commission (2020), *Italy in the Digital Economy and Society Index.*

European Commission (2020), *Latvia in the Digital Economy and Society Index.*

Federal Office For Information Security, (2019),*The State of IT Security in Germany in 2019.*

Federal Office For Information Security, (2020), *The State of IT Security in Germany in 2020.*

Federal Office For Information Security, (2020). *Digitalbarometer: Bürgerbefragung zur Cyber-Sicherheit.*

Government of Ireland (2018), *National Cyber Security Strategy 2019-2024.*

Government of Italy (2020), *Piano Nazionale di Ripresa e Resilienza -PNRR.*

Government of Latvia, (2019), *Informative report, Cybersecurity Strategy of Latvia.*

Government of Latvia, (2020), *Education Development Guidelines 2021-2027 "Future Skills for the Future Society".*

Government of Latvia, (2020), *Digital Transformation Guidelines 2021-2027.*

Guir R. (2002), *Pratiquer les TICE : Former les enseignants et les formateurs à de nouveaux usages*, Bruxelles: De Boeck et Larcier.

Huismann, A. (2020), *Vocational education and training for the future of work: Germany*, Cedefop ReferNet thematic perspectives series.

Information Technology Security Incident Response Institution, (2021), CERT.LV Annual Report 2020.

Izglītības un zinātnes ministrija (2017), *Informatīvais ziņojums "Priekšlikumi konceptuāli jaunas kompetencēs balstītas izglītības prasībām atbilstošas skolotāju izglītības nodrošināšanai Latvijā.*

Izglītības un zinātnes ministrija (2020), *Pedagogiem nodrošināta iespēja bez maksas pilnveidot digitālās prasmes.*

Joseph, V. (2020). *Vocational education and training for the future of work: France*, Cedefop ReferNet thematic perspectives series.

Kultusministerkonferenz (2016), "*Bildung in der digitalen Welt: Strategie der Kultusministerkonferenz"*

Lardellier P., Moatti, D. (2014), *Les ados pris dans la Toile. Des cyberaddictions aux techno-dépendances*, Paris: Éditions Le Manuscrit, Coll. « Addictions : Plaisir, Passion, Possession »

Latvian Safer Internet Centre (Project-platform "Drossinternets.lv"): https://drossinternets.lv/

LIKTA (Latvian Information and Communication Technologies Association): https://likta.lv/digitalasparmainas-izglitiba/

Likumi.lv, Noteikumi par pedagogiem nepieciešamo izglītību un profesionālo kvalifikāciju un pedagogu profesionālās kompetences pilnveides kārtību. https://likumi.lv/ta/id/301572-noteikumi-par-pedagogiem-nepieciesamo-izglitibu-un-profesionalo-kvalifikaciju-un-pedagogu-profesionalas-kompetences-pilnveides

Microsoft Digital Defense Report. https://www.microsoft.com/de-de/security/business/security-intelligence-report.

Ministry of Education, University and Research, Government of Italy, *Piano Nazionale Scuola Digitale – PNSD.*

Ministry of Education, University and Research, Government of Italy, (2018), *La Buona Scuola* (Law No. 107/2015)

Ministry of Education, University and Research, Government of Italy (2020), *Accordo di collaborazione per lo svolgimento di attività didattiche e formative congiunte per promuovere l'educazione alla cittadinanza digitale e l'utilizzo consapevole delle tecnologie digitali e dei social media*, Memorandum of Understanding n. 4 of 28 October 2020.

Ministry of Education, University and Research, Government of Italy (2021), *Innovare e potenziare le competenze digitali nella scuola*, Memorandum of Understanding n. 785 of 22 January 2021.

Ministry of Industry, Trade and Tourism, Government of Spain, Industria Conectada 4.0, Agenda Digital para Espana.

Ministry of Technological Innovation and Digital Transition (2020), *2025 – Strategia per l'innovazione tecnologica e la digitalizzazione del Paese.*

Mokhtar Ben Henda (2016), *Identification des besoins en formation tic/e dans les pays francophones du sud. Étude réalisée par: Initiatives pour le Développement numérique de l'espace universitaire francophone francophone*, [Rapport de recherche] Agence universitaire de la Francophonie.

National Centre for Vocational Education Research, (2020), *Teaching digital skills: Implications for VET educators - good practice guide.*

OECD (2021), Going Digital in Latvia

OECD, (2018), TALIS - The OECD Teaching and Learning International Survey TALIS - OECD Teaching and Learning International Survey

Pridzans, Dzerviniks (2019), *The Topicality of Educators' Digital Competence Development*, SOCIETY. INTEGRATION. EDUCATION Proceedings of the International Scientific Conference. Volume V, May 24th -25th.

Principes et organisation de la deuxième année de la formation des enseignants stagiaires en IUFM, (2002). La circulaire du 4 avril 2002 parue au Bulletin officiel n° 15 du 11 avril 2002.

Saldus Technical School, Study Programme Civil Security and Defence: https://www.saldustehnikums.lv/izglitibas-iespejas/profesijas/profesionala-videja

Stolterman, E (2004), *Information Technology and the Good Life*, International Federation for Information Processing Digital Library; Information Systems Research. Volume 143.

Télé-enseignement : *les 5 risques majeurs en matière de cybersécurité* – Sophos News

Thélot C. (sous la direction) (2004), *Pour la réussite de tous les élèves, rapport officiel de la Commission du débat national sur l'avenir de l'École*, Paris : La documentation Française.

Disclaimer

The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.