Cyber citizen skills and their development in the European Union

Aalto University Research Group

Finland, February 2023

DESCRIPTION SHEET

Publisher and publication date	Aalto University Research Group, January 2023
Authors	Jarno Limnéll, Minna Alasuutari, Niko Candelin, Kaisa Cullen, Oula Halonen, Mika Helenius, Tommi Hermunen, Juha Lappalainen, Sari Latvanen, Marianne Lindroth, Teemu Matilainen, Olli-Pekka Palonen, Janne Riiheläinen, Mirva Salminen, and Pietari Virkkunen
Title	Cyber citizen skills and their development in the European Union
Keywords	Cybersecurity, digital security, civic skills, cyber citizen skills, safety, security, training, education, European Union
Language versions	Finnish, English **Pages** 148

ABSTRACT

The study is part of a larger cyber citizen skills project, the first phase of which is research-based, resulting in this research report. Overall, the project will produce a European model for teaching basic cybersecurity skills and pave the way for its practical implementation, involving the gamification of cyber skills teaching and activities providing regularly updated training material.

The goal of the first phase of the project was to determine the current state of cyber citizen skills education and training in the EU Member States and the kind of educational content available for teaching these skills. The study also examined the national characteristics and requirements of different EU countries regarding cyber citizen skills and the EU's official policies related to the topic. The practical definition of cyber citizen skills is a key part of this research report, as the concept of "cybersecurity" alone has been defined in various ways in different EU countries. In the next project phases, the focus will be on creating EU-wide materials and a web-based game for teaching cyber citizen skills.

An iterative design science approach was chosen for this qualitative study. Various materials were used in the study: documents dealing with cyber citizen skills were used for a background content analysis, qualitative primary data were compiled through a country-specific comparative analysis, and a scoping literature review was used to collect secondary data. The study also includes a game analysis and an assessment of cybersecurity indices.

There is great variation in the basic cybersecurity skills of different EU Member States, and the same applies to the general level of cybersecurity. The key research results indicate a clear will in the EU Member States to build and teach cyber citizen skills. However, national cultural characteristics must be taken into account in pedagogy and the prerequisites for learning must be ensured for different age groups. The continuous development of materials for teaching cyber citizen skills was also considered important because of the continuous development of the cyber operating environment. In addition to being treated as everyday skills and a way to prepare for threats, cyber citizen skills are considered to be enablers in an increasingly digitalised Europe. The games teaching cyber citizen skills that were analysed in this study were fairly simple and linear.

According to the research group's definition, a cyber citizen is a person who permanently or temporarily lives or resides in an EU Member State and uses digital services or directly or indirectly benefits from the provision of such services. The knowledge, skills and abilities required to operate in a cyber environment are jointly called cyber citizen skills. This study also defined sub-areas linked to cyber citizen skills in terms of their content. According to the results of the study, the EU needs a common indicator for the level of cyber citizen skills.

The research group warmly thanks the numerous research participants and EU Member States, whose support was of major importance to the research project's success and for demonstrating the relevant research results.

Contents

1. Introduction

1.1. Background and objectives of the study

Safety and security competence and adequate knowledge about the digital environment and how to operate in it are key elements of safety and security in all our daily lives across Europe. These are civic skills useful to everyone in today's world and in activities that build trust. Everyone needs basic cybersecurity skills, and the development of a safety and security culture based on people's competence and education must be consciously and purposefully promoted.

This research project is based on the practical need to create a safety and security culture for a digital operating environment with people at the core. As is the case in traffic in the physical world, when moving about in the digital world, that is, in the cyber environment, everyone must know the basic rules and procedures in order to operate safely and securely and take advantage of the opportunities on offer. This applies to all age groups. The cyber environment, and technology in general, are constantly evolving, as are the related threats and opportunities. As cyber citizen skills must be constantly developed and updated, the principle of continuous learning and the creation of an appropriate safety and security attitude are important in the development of these skills.

This research paper is the first part of a three-phase implementation plan aimed at creating harmonised cyber citizen skills education and training across the European Union, for all Europeans. The goal of the first phase was to determine the methods, approaches, and materials used to teach cyber citizen skills in all the EU Member States. This included a survey of national pedagogical and cultural characteristics, both from a national perspective and in terms of the European Union's harmonisation requirements. The cybersecurity training offered by universities in the EU Member States was also examined. Higher education institutions build cybersecurity skills that go beyond civic skills, but the number of people educated (and the scope of the programmes they complete) illustrates the pool of instructors capable of educating citizens and, for example, teachers.

This report, resulting from the first phase of the project, focuses on the current state of cyber citizen skills education and training across the European Union and the required substance of cyber citizen skills in the EU. In the second and third phases of the project, this report will be used as the basis for creating a common digital learning portal and a game developing cyber citizen skills. The project relies strongly on research in the first phase, and will then turn to the provision of research-based practical teaching and learning. It is also important to highlight the pedagogical and identified national characteristics of different EU countries during the research phase.

The main research questions of this research report and the research conducted by the Aalto University research group are:

- What is the current state of cyber citizen education in the EU Member States and what kind of educational content is currently available?

- What national characteristics and requirements are related to cyber citizen skills in the different EU countries and the European Union?

- What are the expectations and views of the different EU countries and the European Union with regard to the content and implementation of harmonised cyber citizen education?

The practical definition of cyber citizen skills is a key part of this research report, as the concept of "cybersecurity" alone has been defined in various ways in different countries and by different operators. This has been one of the main starting points of this research report: understanding what knowledge and skills are

associated with cyber citizen skills in different EU countries and what this means in terms of national characteristics.

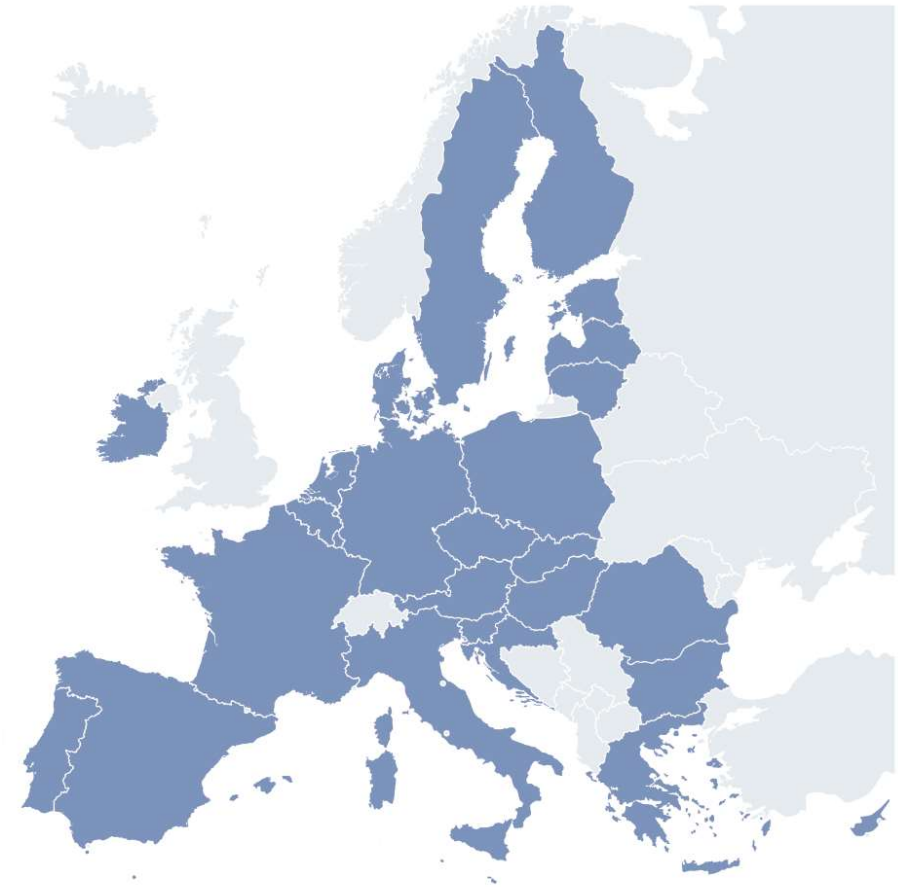

Figure 1: EU countries.

In the context of this study, information was collected from various sources and through personal interviews based on the research questions. The information was collected through direct contacts in EU Member States (authorities and educational institutions), using the networks of the European Union and Finland, as well as the networks of the European Union Agency for Cybersecurity (ENISA). Personal interviews were also an important method of information collection and content analysis as they helped to better understand pedagogical aspects underlying teaching materials. Information collection was carried out systematically using various methods and their combinations. Having collected a comprehensive set of information, the research group evaluated the material both qualitatively and quantitatively, taking into account national characteristics. This helped build an understanding of the basic level of cybersecurity skills and knowledge of EU citizens, as well as the special features of the teaching methods used.

Overall, the project will produce a European model for teaching basic cybersecurity skills and pave the way for its practical implementation, involving the gamification of cyber skills teaching and activities providing regularly updated educational and training material. The project strengthens European cybersecurity and creates common practices and models for Europeans' basic cybersecurity skills. These civic skills are important both now and in the future, and affect all Europeans living in increasingly digital societies. It pays to invest in the teaching and training of these skills while also making use of new kinds of learning methods, such as gamification.

Successfully implementing the project across Europe will improve the security and competitiveness of the European Union in our modern technological world.

1.2. Research methodology

A qualitative research method and an iterative design science approach were chosen for this study. It is based on a variety of materials. It includes cyber citizen skills documents that were used for a background content analysis, qualitative primary data that were compiled through a country-specific comparative analysis, and a scoping literature review that was used to collect secondary data. A game analysis and indices were also used. In addition, a study was conducted on the research, guidance and implementation related to the development of civic cybersecurity skills in the European Union. Secondary data helped assess the suitability of the primary data-based qualitative research for the defined purpose.

The qualitative approach and design science method enabled a broad and in-depth iterative examination of the theme. The method was used to create a firm foundation for the gradual generation of results. The design science method can be used to create reliable solutions to societal issues like the development of civic cybersecurity skills. It helps connect scientific theory and practical activities and boost interaction between the two. Design science is both a process and a continuous, step-by-step problem-solving approach. The gradual creation, continuous evaluation (including suitability and usefulness) and refocusing of outputs generate new insight into the phenomenon studied. Design science is a flexible method that can be applied to solving complex problems.

In the study, information from various materials was mapped, acquired, classified, described, and analysed. Scientific research results must be reliable and relevant. The aim of constructive design science research is to increase practical knowledge, improve operations and generate solutions based on observations. In this design science study, the research process began with a qualitative content analysis that charted the theoretical basis for teaching civic cybersecurity skills in view of its societal relevance.

In design science, the knowledge base for teaching cybersecurity to citizens is developed stepwise by evaluating and refining the results. First, a content review of the existing data and theoretical material was carried out. To refine the results, they were evaluated using a scoping literature review and interview research methods. The constructive research result was evaluated in terms of its relevance and accuracy using numerous critical reviews. This was done by comparing the findings with the collected empirical interview material, written material and educational game analyses.

1.2.1. Definitions

Before initiating the study and the research group's work, the topic was determined by means of a qualitative content analysis. The concept *of cyber citizen skills* has not been clearly defined or specified in different contexts. The analysis of the concepts used in the research project began in February 2022, in connection with the first discussions leading to the research project's launch. During the project, the definition of cyber citizen skills was further refined in collaboration with the project preparers, research group and a number of parties closely involved in the topic. Project meetings gave rise to a very broad and comprehensive definition of cyber citizen skills. The concept's definition was enhanced using the mental map approach. The researchers want the definition to emphasise the broad nature of cybersecurity. The study examined citizens' cybersecurity skills extensively through new and developing threat imagery. A broad definition helped to better deal with an uncertain and complex future in the context of the study. Work on the definition was completed in December 2022, and it is described in Chapter 5.

1.2.2. Methods

This study is a data-driven qualitative study in which several qualitative research methods were used for data collection and validation. It was carried out between March and December 2022 by fourteen researchers and concerned the entire territory of the European Union. The following sources of information were used: background material based on a content analysis, a scoping literature review based on previously published academic research articles, and country-specific analyses based on material from a variety of public sources and thematic interviews. The current state of cybersecurity teaching and training, national and linguistic concepts, emphases, operating models, cybersecurity actors, existing services and games, target groups and the impact of culture from the perspective of the current state and future skills were studied on a country-by-country basis.

The research group represents various perspectives, dimensions, sectors and disciplines of cyber citizen skills. A shared digital workspace was used to store the key EU-related material, project and operator data, game links and evaluation models. At the outset of the project, a platform for collaboration and material was created for the research group, a common source material management method was defined, common research principles were described, a uniform model for country analyses was devised, and a common model for the evaluation of results was refined at the research group's regular meetings. The study relied mainly on primary sources, but secondary sources were used for the countries' overall maturity of cybersecurity. The primary material consisted of interviews, documents, official reports and national reports. For each country, the information obtained from the sources was examined in view of the research questions, the research topic as a whole, the theoretical basis and the research literature.

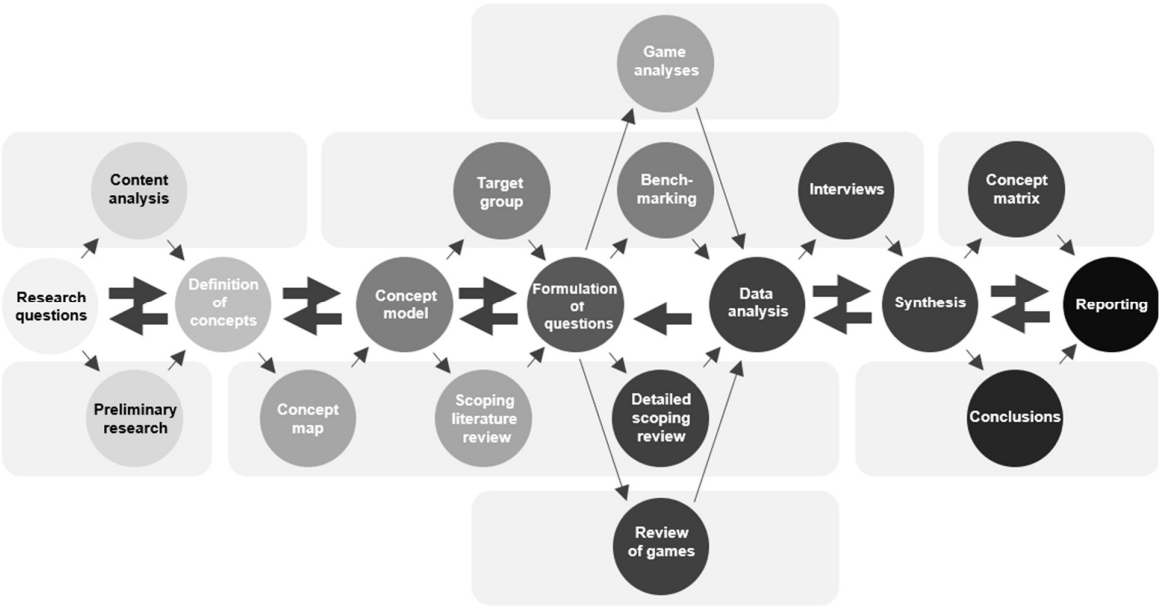

Figure 2: Stages of the iterative research process.

Researchers conducted more than 200 interviews in different EU countries, analysed about 1,000 different websites and surveyed more than 500 different studies, reports or publications. The scope of the literature review is described in Chapter 2.

1.3. Key concepts

Cyberspace

The Ministry of Foreign Affairs of Finland has defined cyberspace to mean the man-made digital parallel reality, which connects people and equipment worldwide across state borders through information technology, automated control systems, the internet and social media.[1]

Regarding the cyber domain, Finland's 2013 Cyber Security Strategy stated that: Threats against the cyber domain have increasingly serious repercussions for individuals, businesses and society in general. The perpetrators are more professional than before and today the threats even include state actors. In addition to cybercrime and economic benefit, cyber attacks can be used to exert political pressure and as an instrument of military influence.[2] Cyberspace is often referred to as a digital operating environment.[3]

Cybersecurity

According to the definition of the Finnish Security Committee, cybersecurity is a target state in which the cyberspace can be trusted and its operation is secured. Cybersecurity refers to the security of a digital and networked society or organisation and its impact on their operations.[4]

Digital security is a term closely related to cybersecurity and is often used to refer to cybersecurity in connection with cyber citizen skills. According to the VAHTI Glossary of Risk Management, digital security is a broader term and refers to "a target state where a digital operating environment can be trusted and operations both there and related to it are secure and managed, even in the event of disruptions"[5]. Digital security can be thought of as an umbrella concept focusing on the digital operating environment, as well as on the various factors that influence the operating environment and the factors that the operating environment influences in turn. Politics and trust, for example, are such factors. The OECD also defines digital security broadly and considers it to include elements such as digital security risk management, continuity management, data protection, data security and cybersecurity. Whereas cybersecurity is taken to be related to national or international security, digital security operates closer to the citizen and can be examined in terms of the goals and actions of individuals. Digital security also includes technical, social and economic aspects.[6]

1.4. Key Indices

In studies, assessments and statistics related to digitalisation and cybersecurity, various frameworks and indices are typically used to measure the maturity and development of the aspects studied. For the comparative analysis of the research material, the research group chose three general indices best suited for the task. Well-established indices commonly used for cybersecurity typically measure national preparedness for cyber attacks, relating the level of preparedness to the target country's degree of digitalisation and emphasising different areas such as valid legislation, training programmes and coordination.

ITU, GCI (Global Cybersecurity Index)

The International Telecommunication Union (ITU) is the United Nations (UN) specialised agency for information and communication technologies (ICT). The Global Cybersecurity Index (GCI), published by the Union since 2015, helps member states identify areas of cybersecurity in need of improvement.

The GCI measures countries' commitment to cyber literacy and awareness-raising. Cybersecurity has an extremely broad scope of application, covering many different industries and sectors. Each country's level of

development or commitment is assessed based on five dimensions: (i) legislative measures; (ii) technical measures; (iii) organisational measures; (iv) capacity building and (v) national cooperation.

The GCI measures legislation and regulatory practices that address cybercrime and cybersecurity, such as acts and decrees implemented to ensure data protection or critical infrastructure security. The index assesses the implementation of technical capabilities (including national CIRTs) in government agencies and sectoral organisations. It measures the implementation of cybersecurity through national strategies and the organisation of activities that implement the strategies. Capacity building is measured based on awareness campaigns, courses, training and incentives to develop cybersecurity. The measurement and assessment of national cooperation capabilities focuses on the Public Private Partnership (PPP), meaning cooperation between public administration and the private sector. The index is formed by combining the results of different areas into an overall score.

To increase cyber citizen skills, security awareness should be improved at the level of citizens, governments and organisations. The GCI measures the inclusion of cybersecurity in national curricula, from primary and secondary education to the academic environment. The index considers individual information security campaigns aimed at companies, the third sector and government agencies, as well as the services available.

The goal of the ITU and the GCI is to promote good practices and develop a global cybersecurity culture and cooperation. The ITU uses the data collected to provide findings and practices that member states can apply in their national activities.[7]

National Cyber Security Index (NCSI)

Established in 2002, the e-Governance Academy (eGA) is a non-profit foundation of the Government of Estonia, the Open Society Institute (OSI) and the United Nations Development Programme. The eGA's mission is to increase the competitiveness of societies in the digital transformation by means of transparency and openness. It produces, develops and maintains the real-time National Cyber Security Index (NCSI).

The NCSI measures the level of preventive cybersecurity in the target countries, including their ability to manage cyber incidents, fight cybercrime, manage and prevent large-scale crises, and develop competence comprehensively. The NCSI focuses on existing and measurable government cybersecurity programs and measures, including: (i) existing legislation (acts, regulations, orders); (ii) established institutions (existing organisations and departments); (iii) forms of cooperation (committees and working groups); and (iv) results (policies, exercises, technologies, websites, and national programmes and implementations). In the assessment, attention is paid to how existing solutions and services relate to denial-of-service attacks, data integrity breaches and data confidentiality breaches. The NCSI consists of a total of 46 indicators, the relative weightings of which are determined by an expert group that convenes annually.

In view of cyber citizen skills, the NCSI assesses education and professional development at different levels of education, including primary and secondary education, first- and second-cycle education, as well as third-cycle education. In addition to educational cooperation, the target countries' ability to identify and analyse cyber threats and produce situational analyses and threat information for their citizens contributes significantly to cyber awareness and resilience, which are closely related to cyber citizen skills. The index also assesses the activities of professional associations and cooperation forums in the field of cybersecurity.

The NCSI's vision is to develop a cybersecurity measurement tool that provides accurate and up-to-date information on cybersecurity in the target countries and related areas of development.[8]

Digital Economy and Society Index (DESI)

The European Commission has been monitoring the Member States' digital development and progress in its Digital Economy and Society Index (DESI) reports since 2014.

DESI is a composite index that summarises indicators relevant to Europe's digital performance and tracks development in EU Member States across five dimensions: (i) connectivity, (ii) human capital, (iii) internet use, (iv) technology integration and use, and (v) digital public services.

The European Commission has specified various indicators, divided into thematic groups, which describe some of the key sectors of the European information society (telecommunications, mobile communications, internet services, eGovernment, eBusiness, ICT training, research and development).

The report combines the quantitative data of DESI indicators in five areas with country-specific policies, related opinions and prevailing practices. The Member States' reports contain country profiles that help Member States specify and identify areas that call for the prioritisation of tasks and allocation of development activities.

DESI measures digital skills in relation to individuals' ability to process and understand information. The index assesses the activity of internet use, users' communication and cooperation skills, and their ability to use digital services. As regards digital skills, it considers the capabilities of content production, as well as skills directly related to problem solving or cybersecurity, including the users' ability to protect the devices they use and the information they process, as well as protect their privacy.[9]

References

[1] "Cyber security and the cyber domain", *Ministry for Foreign Affairs*, accessed on December 27, 2022, https://um.fi/cyber-security-and-the-cyber-domain.
[2] Security Committee, "Finland's Cyber Security Strategy", *Government Resolution of January 24, 2013* (Helsinki: Secretariat of the Security Committee, 2013), 1.
[3] Ministry of Finance, "Digital Security in the Public Sector, Public Sector ICT"*, Publications of the Ministry of Finance – 2020:45* (Helsinki: Ministry of Finance, 2020), 17.
[4] Security Committee, "The Security Strategy for Society", *Government Resolution November 2, 2017* (Helsinki: Secretariat of the Security Committee, 2017), 10, 22.
[5] Digital and Population Data Services Agency, *VAHTI-riskienhallintasanasto digitaaliseen toimintaympäristöön – esittely ja johdatusta, riskiviestintään* (Digital and Population Data Services Agency, 2022), 16.
[6] Digital and Population Data Services Agency*, VAHTI glossary on risk management*, 16, 68.
[7] "Global Cybersecurity Index", *ITU,* accessed on December 1, 2022, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.
[8] "Purpose", NCSI ,accessed on December 1, 2022, https://ncsi.ega.ee/methodology/.
[9] "The Digital Economy and Society Index (DESI)", *European Commission*, accessed on December 1, 2022, https://digital-strategy.ec.europa.eu/en/policies/desi.

2. Cyber citizen skills teaching and training at the EU level and previous research

2.1. Guidance for cyber citizen skills teaching and training and practical measures at the EU level

The goal is to improve cyber citizen skills through EU-level guidance and support for the capacity to develop cybersecurity. Competence development is guided by strategies, policies and frameworks, for example. EU-funded projects also aim to improve cyber literacy in the Union. The European Union Agency for Cybersecurity (ENISA) is responsible for practical measures at the EU level.[10]

2.1.1. Guidance for civic cybersecurity skills training

In 2020, the EU Cybersecurity Strategy published aims to strengthen Europe's resilience against cyber threats and ensure that all citizens and businesses can fully benefit from trustworthy services and digital tools[11]. According to the strategy, around two-fifths of EU citizens have experienced security-related problems and three out of five feel unable to protect themselves from cybercrime. A third of citizens have received fraudulent emails or phone calls, but 83 per cent have never reported a cybercrime. In line with the strategy, the EU's Digital Education Action Plan will raise citizens' cybersecurity awareness, the primary target group being children, young people and organisations (especially SMEs). The strategy also states that cybersecurity skills should be further improved at the EU level through formal education and training (including vocational training), cybersecurity awareness training and cyber exercises. The goal is that all internet users also maintain a global, open, stable and secure cyberspace where everyone can lead a secure digital life[12].[13]

The EU's 2030 Digital Compass sets out the vision and goals for digitalisation by 2030. Dependence on technologies produced outside the EU and on a few large technology companies, as well as the impact of these dependencies on citizens' lives, are mentioned as being problematic in the compass. As stated in the Digital Compass, it is important for the future of Europe and for collective resilience that citizens are digitally skilled and have the necessary basic digital skills. The aim is for 80 per cent of Europe's adult citizens to have at least basic digital skills by 2030. These skills include identifying disinformation and fraud attempts, as well as protecting oneself against cyber attacks and online scams. In addition, it is important for children to learn to navigate through the myriad of information they are exposed to. The objectives of the Digital Compass also state that citizens must respect EU fundamental rights, such as the protection of personal data and privacy, the right to be forgotten and the protection of intellectual property rights in the digital environment.[14]

As stated in the EU Digital Education Action Plan, digital competence is part of the knowledge, skills and attitudes that people need in their lives in accordance with the European Reference Framework of Key Competences for Lifelong Learning. Learning must begin at an early stage and continue throughout people's lives. In addition to technical skills, the teaching of soft skills is considered important. In teaching aimed at developing digital competence, the preference should be for open classrooms, real-life experiences, projects, new learning tools and materials, as well as learning resources open to all. Online collaboration is also encouraged. Digital competences include, for example, critical thinking, media literacy, security skills and privacy-related skills, but teaching these to the wider population is a challenge. Union-wide cooperation is required for peer learning and the exchange of best practices in order to develop education and training in different countries.[15]

The EU has defined digital competence in its DigComp 2.2 framework (The Digital Competence Framework for Citizens). The latest version of the framework, released in 2022, aims to provide a common understanding of

the meaning of digital competence. The DigComp framework has a separate section for safety, but other competencies also include skills that qualify as cyber citizen skills.[16] The competence areas include 1) Information and data literacy, 2) Communication and collaboration, 3) Digital content creation, 4) Safety and 5) Problem solving.[17]

The Safety competence area includes protecting devices and digital content, protecting personal data and privacy in the digital environment, protecting health and wellbeing, being aware of digital technologies that promote social well-being and inclusion, and being aware of the environmental impact of digital technologies and their use.[18] The Problem solving competence area includes identifying problems and needs, resolving conceptual problems and problem situations in digital environments, keeping up-to-date with the digital evolution and using digital tools for innovation. All of these skills are also related to cyber citizen skills.[19] The Communication and collaboration competence area also includes skills related to cyber citizen skills, such as interaction and cooperation in digital channels and digital presence management (digital footprint control and identity and reputation management).[20] As regards the competence area of Information and data literacy, source criticism and life-cycle information management are particularly relevant.[21] Examples of cyber citizen skills in the competence area of Digital content creation include understanding the principles of copyright and being able to use technologies and services in a way that does not jeopardise content or information security.[22]

The EU Cyber Resilience Act (CRA) focuses primarily on strengthening cybersecurity regulation to ensure the security of hardware and software products. However, it also affects citizens, as one of the other general objectives is to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements. Two of the specific objectives of the CRA include enhancing the transparency of security properties of products with digital elements, and enabling businesses and consumers to use products with digital elements securely.[23]

2.1.2. EU organisations and partners involved in the development of cybersecurity skills

The EU Agency for Cybersecurity (ENISA) continues the work of the European Network and Information Security Agency and builds on its structures, but has a stronger role and a permanent mandate. ENISA produces guidelines and reports on the development of cyber citizen skills. In December 2022, it published a report on the state of cyber education (in basic education) in the EU Member States. Based on this report, ENISA will develop a roadmap to guide efforts to increase cybersecurity education in the EU Member States.[24,25]

ENISA is actively involved in cybersecurity education, training, and awareness building. It is primarily responsible for the annual European Cybersecurity Month and produces related material directly for citizens and other operators, as well as organises events. Every year, ENISA organises the European Cyber Security Challenge (ECSC) for young people interested in cybersecurity. The event brings together young people across Europe to network, collaborate and compete. The goal of the ECSC is to encourage young people to pursue a career in cybersecurity by helping them develop their skills and providing contacts in the field.[26] ENISA also organises the International Cybersecurity Challenge (ICC)[27] together with international organisations. The aim of the ICC is to attract young people to the cybersecurity industry and to raise overall awareness of the need for cybersecurity education, training and the skills required in cybersecurity worldwide. The European Cyber Security Skills Framework (ECSF), produced by ENISA,[28] aims to create a common understanding of cybersecurity roles, competencies, skills and knowledge to address the shortage of cybersecurity talent and support the design of cybersecurity education and training programmes. ENISA has also created the Cybersecurity Higher Education Database (CyberHEAD)[29], which lists academic cybersecurity degrees in the EU.

ENISA organises various cybersecurity awareness campaigns targeting EU citizens and organisations. The best known of these is the previously mentioned European Cybersecurity Month, which has an annually changing theme.[30] ENISA also organises the Cyber Health Week, aimed at staff in the healthcare sector and patients.[31] In addition, it organises cybersecurity awareness campaigns for different target groups, as required.[32] ENISA is

currently working on additional material to raise citizens' cybersecurity awareness. The Agency also hosts the recently established Ad-Hoc Working Group on Awareness Raising, which includes people from various stakeholder organisations across Europe. The working group's objectives include developing cybersecurity training and training materials, helping to plan current information campaigns and measuring their effectiveness.[33,34,35]

In 2021, the European Cybersecurity Competence Centre (ECCC) was established in Bucharest, Romania. The European Commission will serve as the Centre's acting Directorate-General while its structures are being created. The Centre will steer the network of national cyber coordination centres in the EU countries and the Union's cybersecurity funding. Its goal is to increase Europe's cybersecurity capacities and competitiveness. In her State of the Union Address in September 2022, the President of the European Commission, Ursula von der Leyen, announced the establishment of a Cybersecurity Skills Academy within the Competence Centre.[36,37]

At the EU level, cybersecurity skills are also developed by the European Cyber Security Organisation (ECSO), which is the European Commission's partner in the implementation of the public-private partnership on cybersecurity. It is a multi-stakeholder, cross-industry partnership bringing together large companies, SMEs and start-ups, research centres, universities, end-users and operators of key services, clusters and associations, and local, regional and national audiences. The ECSO supports the development and benefits of the cybersecurity and ICT security ecosystem (including education, training, and cybersecurity awareness).[38] The Council of European Professional Informatics Societies (CEPIS) aims to provide independent professional expertise concerning IT legislation and cybersecurity topics. The group is also actively involved in other organisations such as ENISA and the ECSO.[39]

At the EU level, cooperation related to the development of cybersecurity also takes place with the United Nations (UN), the Organisation for Security and Cooperation in Europe (OSCE), the North Atlantic Treaty Organization (NATO), the Organisation for Economic Co-operation and Development (OECD), the European Union Agency for Law Enforcement Cooperation (Europol), and especially the European Cybercrime Centre set up by Europol, and the Global Forum of Cyber Expertise (GFCE).[40]

2.1.3. EU projects and measures related to the development of cybersecurity skills

The Digital Europe Programme (DIGITAL) helps the EU achieve a high level of cybersecurity, in line with the Cybersecurity Strategy. It is an investment programme that specifically supports the construction of a European "cyber shield". DIGITAL promotes the wide adoption of the latest security practices and the development of digital skills through its various work programmes. Its aim is to improve resilience, increase risk awareness and improve the basic level of cybersecurity. The project has ongoing work programmes that also include measures affecting EU citizens, such as raising awareness of cybersecurity technologies. DIGITAL's work programme also includes support for higher education in cybersecurity and shorter cyber training, as well as the construction of a platform introducing and mediating education and jobs. This platform, which goes by the name Digital Skills and Jobs Platform, will also provide digital skills training for citizens.[41,42,43]

Cybersecurity Skills Alliance – A New Vision for Europe (REWIRE)[44] is a project aiming to create a concrete European cybersecurity skills strategy for the cybersecurity sector. In particular, the project will develop professional expertise in cybersecurity and provide ways to reduce the skills gap in the field. The project brings together 25 partners across the EU, representing education and training institutions, industry and certification organisations and vocational education and training networks. The REWIRE project builds on the work of four other Horizon2020 cybersecurity projects, namely CONCORDIA, SPARTA, ECHO and CyberSec4Europe.

In the Cyber Security Competence for Research and Innovation (CONCORDIA) project, a cybersecurity network was built to bring together different stakeholders and create a European ecosystem for cybersecurity education and training. Among other things, the project aims to teach cyber skills to professionals, explain cybersecurity issues visually and in an easily understandable way, as well as encourage women to enter the cyber sector. Plans

are to produce cybersecurity teaching material for teachers.[45] The SPARTA project, which has already ended, built a network to develop cybersecurity research, innovation and training with the aim of preventing cybercrime and improving cybersecurity in the EU. Among other things, the project created content for cybersecurity education at universities.[46] The European Network of Cybersecurity Centres and Competence Hub for Innovation and Operations (ECHO) also built a network to develop the cyber sector. The network includes 30 partners from different sectors, including transport, primary production, ICT, education, research, telecommunications, energy, space, healthcare, defence and rescue service. The project has developed the European cybersecurity ecosystem to enable secure cooperation, support the development of the European market and seek ways to protect EU citizens from cyber threats and disruptions.[47] The CyberSec4Europe project designs, tests and demonstrates possible governance structures for the future European Cybersecurity Competence Network, using best practices derived from concepts such as CERN (an organisation formed jointly by Member States, where decision-making power is shared between governmental representatives and representatives of the scientific community) and the expertise and experience of partners. The aim is to improve the security of all EU citizens. Among other things, the project has studied the effectiveness of cybersecurity awareness training. The CyberSec4Europe project ended in December 2022.[48,49]

2.1.4. Training at the EU level

The Digital Skills and Jobs Platform has a page dedicated to cybersecurity training. The site offers citizens free cybersecurity courses, articles related to cyber citizen skills, and guidelines on the topic. The materials of this Cyber Citizen project can also be distributed through the platform.[50,51]

Cyberwiser.eu, funded by the EU, offers courses mainly for professionals or students in the cyber field, but its Primer course is also suitable for people without prior knowledge about cybersecurity. The website contains news and events concerning cybersecurity.[52] The previously mentioned REWIRE project will also publish Vocational Open Online Courses (VOOCs) on its website in late 2023.

The European Union's Learning Corner website offers games and other content for children and young people. The site includes a Cyber Chronix game, a comic strip for teaching cyber skills to young people aged 12–15, a guide on safe online activities for children aged 9–12, and a Happy Onlife game, which provides instructions for staying safe on the Internet and protecting yourself from abuse, for example.[53,54]

2.1.5. The future

Sweden, which holds the Presidency of the Council of the European Union in spring 2023, has announced its intention to increase the security of EU citizens, combat organised crime, protect the EU's values and build a resilient Europe. It intends to continue the strategic programme established with France and the Czech Republic, the previous holders of the Presidency, which specifically aims to combat disinformation and election influencing.[55]

2.2. Observations on previous research

2.2.1. The objective, research question, premise and method of the literature review

Apart from the measures adopted at the EU level, background information for the reports on individual Member States consists of a scoping review of previously published academic research.[56] The review aims to provide information on the kind of research previously conducted on cyber citizen skills education and training, especially in Europe. As "cyber citizen skills" is not an established concept in research, the actual research question and the keywords and phrases used in searches were formulated using more established concepts.

Thus, the research question turned out to be how digital citizenship[57] is understood in academic research, especially in the context of cybersecurity.

The aim of a scoping review is to produce an overview of the scope and depth of existing research based on key publications. It is a general approach that helps identify key concepts and approaches in use and highlight key observations from the relevant research literature. It does not seek to assess the quality of individual studies or to produce a sophisticated analysis of the research field, but focuses specifically on the overall picture.[58] The scoping method enables a literature review to be carried out within the available time and other resources, and in a way that meets the research project's needs.

2.2.2. Description of work

Database searches for the literature review were conducted using various combinations of the keywords listed in Table 1. The AND connector word was used as the Boolean operator. Searches were performed by the title, keywords and abstract of articles. In databases where searches could not be performed by title, keywords and abstract, the entire text was used for the search.

Table 1: Keywords used.

civic* / citizen* / native*	Cybersecurity / "cyber security" / cybersafety / "cyber safety" / "digital security" / "digital safety"	skill* / competen*	train* / educat*
cyber* / digital*	citizen*		

Article searches were performed on six databases (see Table 2). The selection of databases was based on preliminary searches carried out on several databases to assess which of them contained key research articles. The searches focused on six disciplines: educational sciences, social sciences, information technology, management, communication and information research, and psychology. These disciplines were expected to include research related to the teaching of cyber citizen skills. Database searches were limited to articles published in English in or after 2010 that had undergone an evaluation process and were available in the digital collections of Aalto University. This meant that books, chapters of books, conference publications, popular writings and internet sources, for example, were excluded from the search. In practice, the research process proceeded iteratively and flexibly, as search queries, for example, were modified according to the search results, the goal being to obtain as comprehensive a sample as possible from the databases.

Table 2 describes the results obtained from the databases by combining the search terms mentioned above.

Table 2: Search results from different databases.

Database	Search Results	Selected in the 1st round	Selected in the 2nd round
SCOPUS (Elsevier)	995	130	16 from Europe
Springer Link – Springer Compact	270	26	
Science Direct (Elsevier)	172	31	
Business Source Complete (EBSCO)	469	21	

Proquest Databases	924	197	
IEEE Electronic Library IEL (IEEE Xplore)	40	7	
Total	2870	430	

The selections of articles were made by a team of two researchers. The first researcher performed and documented the database searches and made the preliminary article selections based on the title and abstract. The other researcher reviewed the initial selections and read through the articles.[59] In the second step, articles were removed from the sample if, for example, they dealt with digital citizenship but not cybersecurity, or if they focused on parallel phenomena such as teachers' willingness to integrate digital citizenship into their own teaching, citizens' trust in electronic public services, cybercrime or individuals' internet search strategies. The studies are relatively recent. For example, 91 of the 130 articles in the SCOPUS database were published between 2019 and 2022. Due to the limited space available, this report only deals with the 16 articles selected from the SCOPUS database, dealing with European countries.

2.2.3. Key observations from the review

Relatively little research has been carried out on EU citizens' cyber citizen skills. Six of the articles focus on either a single EU Member State (Finland[60], Sweden[61], Bulgaria[62], Poland[63], Greece[64] and Cyprus[65]), an EU Member State and a European non-Member State (the United Kingdom–Ireland–Greece[66] and Spain–the United Kingdom[67]) or the European Union as a whole[68]. When the examination was extended outside the Union, seven more articles focusing on European countries were found (the United Kingdom[69], Turkey[70], Serbia[71] and Russia[72]).

Most of the research focused on children and adolescents, young adults or their educators. Eight of the articles focus on students in higher education, four on teachers/academic staff, three on schoolchildren/children or young people, two on the population overall and one on both the unemployed and retirees. One of the studies is an analysis of written material.[73] Educational institutions and teachers are considered to play an important role in educating competent digital citizens. This means that teachers' digital and cybersecurity skills will be of great importance[74] – as will curricula, which as yet do not adequately account for digital competence[75], and differences between schools in terms of their internal policies and provision of necessary equipment, software and connections for pupils, students and teachers[76]. However, the teaching of digital citizenship in educational environments and its research do not reveal much about the cyber citizen skills of the entire population. This is especially true of those who went to school before digitalisation changed nearly every aspect of their lives and who have learned digital skills independently, with the help of family and friends, in different courses or in training organised by their employer.

The research methods used in the articles are diverse, including mixed methods research, development research, action research, interview research and target group interviews, association rule mining, statistical analysis, literature reviews, document analysis and explanatory mixed method approaches. Most of the research data (half of the articles) were collected using self-assessment forms sent or given to the informants. One of the articles focuses solely on the process of creating such a self-assessment form.[77] Although self-assessments do not give an accurate picture of, for example, the cybersecurity competence of the research subjects, it is often a successful way of gathering information about people's experiences, needs and activities that can be used in different contexts.[78]

Much of the research focuses on people's digital and cybersecurity awareness and behaviour. Things that everyone should see to, such as passwords, digital footprints, sensible sharing of personal data, antivirus protection and privacy settings, are often discussed under the general heading of security. One of the articles lists expected behaviour related to digital security, rights and obligations, and the law, and focuses on digital

security competence in two areas: personal precautions and technical precautions.[79] In general, the kinds of cyber citizen skills that are taught or should be taught and how this is or should be done is not discussed much in previous research. A study of the learning of computational thinking is the only one that (1) considers computational thinking to be a civic skill and (2) clearly addresses the problem of how to teach computational thinking to students who are not yet adequately capable of abstract thinking. In this case, game playing and game editing gave promising preliminary results.[80]

A study that focused on the entire European Union and knowledge of data protection legislation defined four types of digital citizens: the off-line citizens (lowest ranking in internet use and GDPR awareness), the web citizens (average ranking in internet use and GDPR awareness), the social netizens (highly active social media use but low GDPR awareness) and the data citizens (highest ranking in internet use and GDPR competence).[81] Digital citizenship has also been categorised along the lines of (1) source criticism and critical thinking, (2) ethical, safe and faultless use of digital technologies, and (3) material and immaterial means of democratic participation.[82] Technology mastery (competencies, abilities, skills) has been defined as a separate area from digital citizenship (attitudes and behaviours).[83] In some cases, digital skills have been considered to include skills that promote the creative, critical, safe, ethical and responsible use of information and communication technologies to achieve a given objective. They also mean the ability to adapt to new knowledge and an attitude that ensures success in today's digital environment.[84] One of the studies clearly highlighted digital human rights and the importance of training provided by employers[85], while another one considered people's reluctance to change their own behaviour or learn more about cybersecurity, even if they realise their data are not safe[86].

2.2.4. Digital citizenship and cybersecurity

Digital citizenship usually refers to an individual's opportunities and abilities to use digital technology to participate in society. Conceptualization encompasses an individual's skills, knowledge, attitudes, and behaviour.[87] When using digital citizenship as a theoretical framework, the models proposed by Ribble et al. and Choi et al. are the most popular.[88]

In the model of Ribble et al., digital citizenship consists of nine elements. These are: etiquette (models of behaviour and action), communication (electronic exchange of information), education (learning and teaching technology and its use), inclusion (participation in the digital society), commerce (electronic buying and selling), rights (universal freedoms in the digital environment), safety (physical and mental wellbeing) and security (self-protection, that is, measures to ensure one's own security). The model emphasises the moral behaviour of individuals and, at its simplest, defines digital citizenship as norms of behaviour that guide the use of information and communication technologies.[89]

There are two slightly different versions of the digital citizenship model of Choi et al. In the first one, digital citizenship consists of four areas. These include ethics (internet users' commitment to safe, ethical and responsible internet behaviour), media and information literacy (users' access to the internet and digital services, and their ability to assess information, communicate and collaborate with others), participation/engagement (using the internet for political, economic, social or cultural activities) and critical resistance (participation that promotes change, challenges existing power relations and promotes social justice). These areas form the basis for the other model, the digital citizenship scale, which can be used to assess an individual's level of digital citizenship. The five main components of the scale are political activity on the Internet, technical skills, local/global awareness, critical approach and agency in networks.[90]

The framework of several European studies consists of DigComp[91] or DigComp in combination with another framework[92]. As a rule, various aspects of cybersecurity or safety, including data protection and privacy, critical thinking or practical and technical information security measures, are only part of the overall framework of digital citizenship. Safety is usually closely related to the responsibilities of individuals or to the expected – often moral – behaviour. However, the definitions of civic skills required in the digital environment vary, and there is

no reliable way to measure them.[93] More research is thus required on the learning and teaching of cyber citizen skills and their development.

References

[10] A personal communication to the researcher, 21/07/2022.
[11] "Cybersecurity: how the EU tackles cyber threats", *Council of the European Union*, accessed on June 20, 2022, https://www.consilium.europa.eu/en/policies/cybersecurity/.
[12] European Commission, *The EU's Cybersecurity Strategy for the Digital Decade* (Brussels: European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2020), 2, 12, 25.
[13] A personal communication to the researcher, 31/08/2022.
[14] European Commission, *2030 Digital Compass: the European way for the Digital Decade* (Brussels: European Commission, 2021), 1–4, 13.
[15] European Commission, *The Digital Education Action Plan* (Brussels: European Commission, 2018), 1–4, 7.
[16] Riina Vuorikari, Stefano Kluzer and Yves Punie, *DigComp 2.2: The Digital Competence Framework for Citizens*, EUR 31006 EN (Luxembourg: Publications Office of the European Union, 2022), 2.
[17] Vuorikari et al., *DigComp 2.2*, 3. In the Framework, citizens' cybersecurity competences are referred to as Safety rather than Security, which can lead to confusion. The terms are not equivalent.
[18] Vuorikari et al., *DigComp 2.2*, 37–42.
[19] Vuorikari et al., *DigComp 2.2*, 43-50.
[20] Vuorikari et al., *DigComp 2.2*, 15-26.
[21] Vuorikari et al., *DigComp 2.2*, 13-14.
[22] Vuorikari et al., *DigComp 2.2*, 27-28.
[23] European Commission, *Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020* (Brussels: European Commission, 2022), 1–2.
[24] "Cybersecurity Education Initiatives in the EU Member States", *ENISA*, accessed on December 21, 2022, https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states.
[25] A personal communication to the researcher, 06/10/2022.
[26] "European Cyber Security Challenge (ECSC)", *ENISA*, accessed on October 8, 2022, https://www.enisa.europa.eu/topics/education/eu-cyber-challenge.
[27] "International Cybersecurity Challenge (ICC)", *ENISA*, accessed on October 8, 2022, https://www.enisa.europa.eu/topics/education/international-cybersecurity-challenge-icc.
[28] "ECSF European Cybersecurity Skills Framework", *ENISA*, accessed October 7, 2022, https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.
[29] "CYBERHEAD – Cybersecurity Higher Education Database", *ENISA*, accessed on October 9, 2022, https://www.enisa.europa.eu/topics/education/cyberhead#/.
[30] "European Cybersecurity Month", *ENISA*, accessed on October 29, 2022, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/european-cyber-security-month.
[31] "Cyber Health Week", *ENISA*, accessed on October 30, 2022, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals.
[32] "Cyber Energy Week", *ENISA*, accessed on November 26, 2022, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/cyber-energy-week. For example, in 2022, a Cyber Energy Week campaign was organised for those working in and with the energy sector.
[33] A personal communication to the researcher, 06/10/2022.
[34] A personal communication to the researcher, 21/07/2022.
[35] A personal communication to the researcher, 31/08/2022.
[36] A personal communication to the researcher, 22/09/2022.
[37] A personal communication to the researcher, 08/12/2022.
[38] "Europan Cyber Security Organisation", *ECSO*, accessed on April 29, 2022, http://www.ecs-org.eu/.
[39] "Council of European Professional Informatics Societies", *CEPIS*, July 15, 2022, https://cepis.org/.
[40] A personal communication to the researcher, 20/06/2022.
[41] A personal communication to the researcher, 09/09/2022.
[42] "Digital Skills and Jobs Platform", *European Union*, accessed on September 10, 2022, https://digital-skills-jobs.europa.eu/en.
[43] European Commission, *Commission Implementing Decision on the financing of the Digital Europe Programme and the adoption of the multiannual work programme for 2021–2022* (Brussels: European Commission, 2021), 98, 106–110.
[44] "Cybersecurity Skills Alliance", rewire ,accessed on August 18, 2022, https://rewireproject.eu/.
[45] "Concordia", *CONCORDIA*, accessed on August 18, 2022, https://www.concordia-h2020.eu/.
[46] "Cybersecurity training and awareness", *SPARTA*, accessed on August 19, 2022, https://www.sparta.eu/training/.
[47] "The European network of Cybersecurity Centres and Competence Hub for Innovation and Operations", *echo*, August 19, 2022, https://echonetwork.eu/.
[48] "Cyber Security for Europe", *CyberSec4Europe*, accessed on August 19, 2022, https://cybersec4europe.eu/.
[49] A personal communication to the researcher, 16/08/2022.
[50] A personal communication to the researcher, 09/09/2022.
[51] "Cybersecurity", *Digital Skills & Jobs Platform*, accessed on October 1, 2022, https://digital-skills-jobs.europa.eu/en/cybersecurity.
[52] "Cyberwiser.eu," accessed on October 15, 2022. https://www.cyberwiser.eu/.
[53] A personal communication to the researcher, 09/09/2022.
[54] "Learning corner", *European Union*, accessed on September 11, 2022. https://learning-corner.learning.europa.eu/index_en.

[55] "Sweden's Presidency of the Council of the EU", *Government Offices of Sweden*, accessed on November 29, 2022. https://www.government.se/government-policy/swedens-eu-presidency-2023/.
[56] E.g. Andrew Booth, Anthea Sutton and Diana Papaioannou, *Systematic Approaches to a Successful Literature Review*, 2nd ed. (London: SAGE, 2016); Danielle Levac, Heather Colquhoun and Kelly K O'Brien, "Scoping studies: advancing the methodology", *Implementation Science* 5, no. 69 (2010), doi: 10.1007/9781748-5908-5-69.
[57] E.g.Moonsun Choi, "A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age", *Theory & Research in Social Education* 4, no. 4/2016 565-607, doi: 10.1080/00933104.2016.1210549; Moonsun Choi, Michael Glassman and Dean Cristol, "What it means to be a citizen in the internet age: Development of a reliable and valid digital citizenship scale", *Computers and Education* 107 (2017): 100-112, doi: 10.1016/j.compedu.2017.01.002.
[58] Booth et al., *Systematic Approaches*, 23, 38, 84.
[59] See Levac et al., "Scoping Studies", 5–6.
[60] Maiju Kyytsönen, Jonna Ikonen, Anna-Mari Aalto and Tuulikki Vehko, "The self-assessed information security skills of the Finnish population: A regression analysis", *Computers and Security* 118 (2022): 102732, doi: 10.1016/j.cose.2022.102732.
[61] Alex Örtegren, "Digital Citizenship and Professional Digital Competence – Swedish Subject Teacher Education in a Postdigital Era", *Postdigital Science and Education* 4: 467-493, doi: 0.1007/s42438-022-00291-7.
[62] Valentina Milenkova and Vladislava Lendzhova, "Digital Citizenship and Digital Literacy in the Conditions of Social Crisis", *Computers* 10, no. 40 (2021), doi: 10.3390/computers10040040.
[63] Aleksandra Pawlicka, Renata Tomaszewska, Ewa Krause, Dagmara Jaroszewska-Choraś, Marek Pawlicki and Michał Choraś, "Has the pandemic made us more digitally literate? Innovative association rule mining study of the relationships between shifts in digital skills and cybersecurity awareness occurring while working remotely during the COVID-19 pandemic", *Journal of Ambient Intelligence and Humanized Computing*, online ahead of printing, doi: 10.1007/s12652-022-04371-1.
[64] Marianthi Grizioti and Chronis Kynigos, "Code the mime: A 3D programmable charades game for computational thinking in MaLT2", *British Journal of Educational Technology* 52 (2021): 1004-1023, doi: 10.1111/bjet.13085.
[65] Hasan Tangül and Emrah Soykan, "Comparison of Students' and Teachers' Opinions Toward Digital Citizenship Education", *Frontiers in Psychology* 12 (2021): 752059, doi: 10.3389/fpsyg.2021.752059.
[66] Konstantina Martzoukou, Crystal Fulton, Petros Kostagiolas and Charilaos Lavranos, "A study of higher education students' self-perceived digital competences for learning and everyday life online participation", *Journal of Documentation* 76, no. 6/2020 1413-1458, doi: 10.1108/JD-03-2020-0041.
[67] Mark Thomas Peart, Prudencia Gutiérrez-Esteban and Sixto Dubo-Delgado, "Development of the digital and socio-civic skills (DIGISOC) questionnaire", Education Technology Research and Development 68 (2020): 3327-3351, doi: 0.1007/s11423-020-09824-y.
[68] Rćzvan Rughiniș, Cosima Rughiniș, Simona Nicoleta Vulpe and Daniel Rosner, "From social netizens to data citizens: Variations of GDPR awareness in 28 European countries", *Computer Law and Security Review* 42 (2021): 105558, doi: 10.1016/j.clsr.2021.105585.
[69] Konstantina Martzoukou, Petros Kostagiolas, Charilaos Lavranos, Thorsten Lauterbach and Crystal Fulton, "A study of university law students' self-perceived digital competences", *Journal of Librarianship and Information Science* 54, no. 4/2021 1-19, doi: 10.1177/09610006211048004; D. McGillivray, G. McPherson, J. Jones and A. McCandlish, "Young people, digital media making and critical digital citizenship", *Leisure Studies* 35, no. 6/2016 724–738, doi:10.1080/02614367.2015.1062041.
[70] Filiz Elmali, Ahmet Tekin and Ebru Polat, "A Study on Digital Citizenship: Preschool Teacher Candidates vs. Computer Education and Instructional Technology Teacher Candidates", *Turkish Online Journal of Distance Education* 21, no. 4 (October 2020): 251–269; Ridvan Ata and Kasim Yildirim, "Turkish Pre-service Teachers' Perceptions of Digital Citizenship in Education Programs", *Journal of Information Technology Education: Research* 18 (2019): 419-438, doi: 10.28945/4392; Nuri Kara, "Understanding University Students' Thoughts and Practices about Digital Citizenship: A Mixed Methods Study", *Educational Technology and Society* 21, no. 1/2018 172–185, http://www.jstor.org/stable/26273878.
[71] Ana Kovačević, Nenad Putnik and Oliver Tošković, "Factors Related to Cyber Security Behavior", *IEEE Access* 8 (2020): 125140-125148, doi: 10.1109/ACCESS.2020.3007867.
[72] L.V. Astakhova, "Issues of the Culture of Information Security under the Conditions of the Digital Economy", *Scientific and Technical Information Processing* 47, no. 1/2020 56-64, doi: 10.3103/S0147688220010062.
[73] Astakhova, "Issues of the Culture".
[74] For example, McGallivray et al., "Young people", 724; Martzoukou et al., "A study of university law", 3; Örtegren, "Digital citizenship", 471, 479, Martzoukou and others., "A study of higher education", 1419, consider teachers' digital and cybersecurity skills to be deficient. Instead, Elmali et al., "A Study on Digital Citizenship," 262, concludes that teacher students' level of digital competence is above average.
[75] Martzoukou et al., "A study of higher education", 1418, 1434; Elmali et al., "A Study on Digital Citizenship", 264.
[76] McGallivray et al., "Young people", 724; Örtegren, "Digital citizenship", 471, 480.
[77] Peart et al., "Development of the digital".
[78] Marzoukou et al., "A study of university law", 6.
[79] Elmali et al., "A Study on Digital Citizenship", 253–254, 264.
[80] Grizioti and Kynigos, "Code the mime".
[81] Rughiniș R. et al., "From social netizens to data citizens".
[82] Örtegren, "Digital citizenship", 480; McGallivray et al., "Young people".
[83] Martzoukou et al., "A study of higher education", 1419, 1436.
[84] Peart et al., "Development of the digital", 3329.
[85] Pawlicka et al., "Has the pandemic made us".
[86] Kovačević et al., "Factors Related to Cyber", 125147.
[87] Örtegren, "Digital citizenship", 470.
[88] Örtegren, "Digital citizenship"; Elmali et al., "A Study on Digital Citizenship"; Martzoukou et al., "A study of higher education"; Tangül and Soykan, "Comparison of Students"; Milenkova and Lendzhova, "Digital Citizenship"; Kara, "Understanding University Students"; Ata and Yıldırım, "Turkish Pre-Service Teachers".

[89] E.g. Mike S. Ribble, Gerald D. Bailey and Tweed W. Ross, "Digital Citizenship. Addressing Appropriate Technology Behavior*", Learning & Leading with Technology* 32, no.1 (2004): 6–11, https://files.eric.ed.gov/fulltext/EJ695788.pdf. (19 December 2022); Mike S. Ribble and Gerald D. Bailey, *Digital citizenship in schools: Nine elements all students should know* (Washington DC: International Society for Technology in Education, 2007).
[90] Choi, "A Concept Analysis"; Choi et al., "What it means to be a citizen".
[91] Riina Vuorikari, Stefano Kluzer and Yves Punie, DigComp 2.2: The Digital Competence Framework for Citizens, EUR 31006 EN (Luxembourg: Publications Office of the European Union, 2022).
[92] Martzoukou et al., "A study of higher education"; Marzoukou et al., "A study of university law;" Örtegren, "Digital Citizenship"; Peart et al., "Development of the digital"; Pawlicka et al., "Has the pandemic made us". Milenkova and Lendzhova, "Digital Citizenship," refer to the publications forming the background for DigComp.
[93] Peart et al., "Development of the digital", 3329.

3. Analyses of individual countries

3.1. The Netherlands

ITU, Global Cybersecurity Index (GCI) 2020	16/182 (Global), 10/46 (Europe)
National Cyber Security Index (NCSI) 2022	18/160 (24 October 2022)
The Digital Economy and Society Index (DESI, 2022)	3/27

3.1.1. Strategic cyber education and training policies

In 2022, the Dutch government published its 2022–2028 National Cyber Security Strategy 2, From awareness to capability. The strategy includes an action plan with concrete actions to improve digital security in the Netherlands. In the Cyber Security Strategy, the Government describes its vision of the digital society and the role and responsibilities of the government, businesses and citizens in it. The strategy has four main objectives. The first objective is to increase the digital resilience of government, businesses and civil society organisations. The second objective is to provide safe and innovative digital products and services across the country. The third objective is to fight the digital threats posed by other states and criminals. The fourth objective is to ensure an adequate number of cybersecurity professionals, develop training on digital security, and increase citizens' preparedness and resilience to digital threats.[94,95]

To achieve the objectives of the latest Cyber Security Strategy, the system of digital security and training for both businesses and Dutch citizens will be strengthened. The National Cyber Security Centre (NCSC), the Digital Trust Centre (DTC) and the Cyber Security Incident Response Team for Digital Service Providers (CSIRT-DSP) will be merged into a single national cybersecurity authority. The national cybersecurity authority is tasked with understanding the vulnerabilities and threats of the digital world. In addition, the data of the various parties will be interlinked through information sharing between the public and private sectors. One of the goals is also to prevent harm to society and mitigate threats. The research cluster contributes to these objectives by evaluating scientific innovations and identifying relevant research questions. The research programme has four themes: crisis management, risk management, strategic and social aspects of cybersecurity, and technology and cybersecurity (technological innovations). The aim of these themes is to enhance cybersecurity training. [96,97,98]

3.1.2. The current state of cyber citizen skills education and training

The reform of primary and secondary school curricula has continued for several years in the Netherlands. The focus is on creating a structured place for digital literacy throughout the curriculum in balance with other learning objectives. In 2022, a national curriculum development institute (Stichting Leerplanontwikkeling, SLO) was established as a non-profit organisation. The SLO has defined the content – knowledge, skills, and attitude – for digital literacy just like for other areas of basic education. The related frameworks are divided into different areas: 1) studying the internet in a secure environment, 2) understanding the importance of acting carefully in social networks and deliberately on the internet, 3) using secure passwords and understanding their importance, 4) safely handling information shared by others, and 5) being aware of cookies, bots and GPS trackers. The goal is for the enhanced digital literacy education to be a reality from the academic year 2024/2025.[99]

The national cybersecurity authority is tasked with launching projects with research institutes such as the Netherlands Organisation for Applied Scientific Research TNO (Nederlandse Organisatie voor Toegepast

Natuurwetenschappelijk Onderzoek) and the Research and Documentation Centre WODC (Wetenschappelijk Onderzoek- en Documentatiecentrum). The cybersecurity authority also participates in various studies by sharing information, mentoring postgraduate students and doctoral candidates and organising lectures. It evaluate research proposals related to the projects and themes to which it is committed in its role as the cybersecurity authority. The TNO organises cybersecurity training webinars for companies and public organisations. The WODC conducts independent scientific research or commissions recognised institutes and universities to do so.[100,101]

The campus of the Hague University is home to The Hague Security Delta (HSD). More than 275 companies, government organisations and knowledge institutes have been working together since 2013 to help secure an increasingly digitised society. The HSD is a non-profit organisation that shares its knowledge and collaborates on innovative security solutions that can be scaled within the Netherlands and internationally. The HSD "thinks, dares and acts" by providing access to knowledge, innovation, markets, finance and talent in the cybersecurity industry. It organises cybersecurity programmes, training and events, including international ones.[102] In 2016, the HSD published an agenda for human capital cybersecurity (Human Capital Actie Agenda Cyber Security 2016–2018).[103] In this connection, it also launched the website securitytalent.nl.[104] The goal is to address the shortage of cybersecurity professionals. The agenda aims to achieve the following objectives: Firstly, more training will be provided to increase the number of teachers. Secondly, connections will be strengthened to adapt to the needs of training programmes and business needs. Thirdly, the sector's appeal will be boosted to attract cybersecurity students. Fourthly, the competence of cybersecurity professionals will be further improved. In addition, training programmes will be encouraged to increase talent in the cybersecurity sector.

The Indo-Dutch Cyber Security School 2022 (IDCSS) offers 20 lectures on a wide range of cybersecurity-related topics by renowned experts, as well as the opportunity to work on real case studies provided by leading Dutch and Indian organisations.[105] Master's degrees in cybersecurity are offered by the following universities in the Netherlands: University of Amsterdam, Security and Network Engineering[106]. Vrije Universiteit Amsterdam, Computer Security[107]. Radboud University Nijmegen, Cyber Security[108] and Computing Science[109]. Leiden University, Intelligence and National Security[110], Cybersecurity Governance[111], Crisis and Security Management[112] and Cyber Security[113]. University of Twente and TU Delft, 4TU Cybersecurity Master Specialization[114]. Eindhoven University of Technology, Information Security Technology track[115].

Cybersecurity games specifically aimed at children and young people are available in the Netherlands. Hackshield is a cybersecurity game for 8-12-year-olds developed by the Centre for Crime Prevention and Safety (Centrum voor Criminaliteitspreventie en Veiligheid, CCV). The website also contains a database of municipal cyber projects for different age groups and communities. Children learn to confront cybersecurity threats in the digital world in a playful way and are encouraged to pass on what they learn to their parents and grandparents. Municipalities play an important role in the project. The mayor sends a video message inviting children to play the game and become junior cyber agents. Later, the mayor pays tribute to the children in person, further motivating them to apply what they have learned.[116] Cyber24, an escape game, is aimed at children and young adults aged 12-21. It has been developed by Mooveteam in collaboration with the Dutch police and cybersecurity professionals. The game teaches the players how their online behaviour affects their cybersecurity and what consequences this may have. Cyber24 is a modern interactive escape game dealing with various topics such as sexual harassment, identity theft, money scams, social media scams and hacking. During the escape experience, players work in small groups to prevent the characters of the story falling victim to online crime. In this way, they play the roles of both "perpetrator" and "victim" and experience both sides themselves. They can see the effects of their actions, as well as changes in their attitudes and behaviours. The post-game interview ensures that experiences are shared and knowledge is better refined. In short, Cyber24 is a unique combination of playing and learning.[117]

The Netherlands Cyber Security Awareness Training e-Learning Course Sample is an interactive module with 3D-based cybersecurity risk simulations.[118] It has been produced by the Ministry of Compliance (Opleidingen van

Charco & Dique).[119] The module challenges the player to engage in real-life scenarios, increasing cybersecurity awareness and demonstrating the importance of positive cybersecurity behaviour. The application of a game-like challenge in cybersecurity training experiences can significantly improve the ability to acquire new cybersecurity skills and observe cyber risks. Gamification uses kinetic movement instead of rote memorisation, offering the player a positive learning experience in a safe environment.

The annual Cybersecurity Month is organised in October by SIDN (Stichting Internet Domeinregistratie Nederland), which manages the Dutch domains and domain names. The aim of the annual Cybersecurity Month is to promote cybersecurity awareness in public and private sector organisations and to provide training courses and exercises. The goal is to encourage the organisations' employees, customers and contacts to think about cybersecurity through fun activities such as pub quizzes or quizzes for organisations and teams. Updated information about the current state of cybersecurity and tools related to cybersecurity topics are also shared.[120,121] The Cybersecurity Week took place in the Hague from 17 to 21 October 2022. It is organised by the HSD around the same time every year. The Cybersecurity Week takes place during the European Cybersecurity Month. It is the EU's annual information campaign, which takes place across Europe in October. The aim is to raise awareness of cybersecurity threats and promote cybersecurity among citizens and organisations.[122] Safer Internet Centre Nederland is part of the European Better Internet for Kids programme. It develops materials and activities with the government, businesses and societal institutions and provides young people and their social networks, including parents, teachers and care providers, the tools they need to become digitally skilled citizens.[123,124]

3.1.3. National characteristics

To improve cybersecurity, three cybersecurity clusters in the Netherlands have been merged into a single cybersecurity authority. This was done to improve access to information and its sharing between the public and private sectors, as well as to invest in research and innovation. In addition, efforts are made to ensure the required number of experts with the provision of adequate training and to develop citizens' capabilities and resilience in preparing for cybersecurity threats. Europol's European Cybercrime Centre (EC3) is located in The Hague. The Dutch Cyber Security Strategy aims to move from awareness to the next level, that is, capability. The goal is for software and hardware to be cyber secure to start with.[125]

3.1.4. The definition of cyber citizen skills

The Netherlands does not have a specific definition of cyber citizen skills. The definition of "civic competences" is based on the content of training packages for citizens, which focus on the basic skills that citizens need in the digital world to contribute to their own safety and that of others. The skills are based on the previously discussed SLO frameworks. Emphasis is also placed on everyone's individual responsibility, which can have an impact on other people's cybersecurity. Everyone must understand the importance and basic principles of protecting their own personal data and devices. The goal is to understand the risks and threats of the digital environment (including malware, social manipulation and identity theft) and to be familiar with the necessary measures (such as the use of antivirus software and a network firewall).

References

[94] Minister of Justice and Security, *National Cyber Security Strategy 2, From awareness to capability* (2022).
[95] "Cabinet presents new cybersecurity strategy," *Government of the Netherlands,* accessed on February 9, 2023, https://www.government.nl/latest/news/2022/10/10/cabinet-presents-new-cybersecurity-strategy.
[96] "National Cyber Security Centrum (NSCs)", *Ministerie van Justitie en Veiligheid*, accessed on October 29, 2022. https://www.ncsc.nl/.
[97] "Digital Trust Center", *Ministerie van Economische Zaken en Klimaat*, accessed on November 22, 2022. https://www.digitaltrustcenter.nl/.
[98] "CSIRT-DSP", *Ministerie van Economische Zaken en Klimaat,* accessed on November 19, 2022. https://www.csirtdsp.nl/.
[99] A personal communication to the researcher, 19/07/2022.
[100] "Towards Digital Life: Een toekomstvisie op AI anno 2032", *TNO*, accessed on November 26, 2022. https://www.tno.nl/nl/.
[101] "WODC," *Wetenschappelijk Onderzoek- en Documentatiecentrum*, accessed on November 26, 2022. https://www.wodc.nl/.
[102] "The Dutch security cluster", *HSD*, accessed on November 26, 2022. https://securitydelta.nl/.
[103] The Hague Security Delta, *Human Capital Actie Agenda Cyber Security 2016–2018*, (2016).
[104] "Security Talent", *HSD*, accessed on 6 December 2022, https://securitytalent.nl/.
[105] "Indo Netherlands Cyber Security School 2022", *HCSS*, accessed on November 26, 2022. https://www.youtube.com/watch?v=jkNbbm2OYCA.
[106] "Master Education SNE/OS3", Security & Network Engineering, accessed on November 30, 2022. https://www.os3.nl/.
[107] "Build tomorrow's hacker-proof computer systems", *Vrije Universiteit Amsterdam*, accessed on December 8, 2022. https://vu.nl/nl/onderwijs/master/computer-security.
[108] "Master Cyber Security", *Radboud Universiteit*, accessed on December 8, 2022. https://www.ru.nl/opleidingen/masters/cyber-security.
[109] "Bachelor Informatica", *Radboud Universiteit*, accessed on December 8, 2022. https://www.ru.nl/opleidingen/bachelors/informatica.
[110] "Intelligence and National Security (MSc)", *Universiteit Leiden,* accessed on December 8, 2022. https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management/intelligence-and-national-security.
[111] "Cybersecurity Governance (MSc)", *Universiteit Leiden*, accessed on December 8, 2022. https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management/cybersecurity-governance.
[112] "Crisis and Security Management (MSc)", *Universiteit Leiden,* accessed on December 8, 2022. https://www.universiteitleiden.nl/en/education/study-programmes/master/crisis-and-security-management.
[113] "Cyber Security (MSc)", *Universiteit Leiden,* accessed on December 8, 2022. https://www.universiteitleiden.nl/en/education/study-programmes/master/cyber-security.
[114] "4TU.Cyber Security", *4TU*.Federation, accessed on November 30, 2022. https://www.4tu.nl/cybsec/.
[115] "Master track in cyber security, Information Security Technology", *Eindhoven University of Technology track*, accessed on November 30, 2022, https://ist.win.tue.nl/.
[116] "Hackshield", *CCV*, accessed on October 27, 2022. https://hetccv.nl/onderwerpen/cybercrime/database-lokale-cyberprojecten/hackshield/.
[117] "Cyber24", *CCV*, accessed on October 27, 2022. https://hetccv.nl/onderwerpen/cybercrime/cyber24/.
[118] "Dutch (Nederlands) - Cybersecurity Awareness Training e-Learning Course Sample", *Security Quotient*, accessed on December 3, 2022. https://www.youtube.com/watch?v=fuse2GVw15I.
[119] "Laws and regulations translated into practice", *Ministry of Compliance, opleidingen van Charco & Dique*, accessed on December 5, 2022. https://www.ministryofcompliance.nl/en/.
[120] "SIDN and .nl registrars support Cybersecurity Month in October", *SIDN*, accessed on October 27, 2022. https://www.sidn.nl/en/news-and-blogs/sidn-and-nl-registrars-support-cybersecurity-month-in-october.
[121] "Zorgeloos online", *SIDN*, accessed on November 26, 2022. https://www.sidn.nl/.
[122] "Cyber Security Week in the Haque", *The Hague & Partners,* accessed on November 26, 2022. https://www.cybersecurityweek.nl/.
[123] "SiC Nederland Safer Internet Centre", accessed on October 18, 2022. https://saferinternetcentre.nl/.
[124] "Safer Internet Forum 2022", *Better Internet For Kids*, accessed on October 28, 2022. https://www.betterinternetforkids.eu/policy/safer-internet-forum.
[125] Minister of Justice and Security, *National Cyber Security Agenda: A cyber secure Netherlands* (2018).

3.2. Belgium

ITU, Global Cybersecurity Index (GCI) 2020	19/182 (Global), 12/46 (Europe)
National Cyber Security Index (NCSI) 2022	3/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	16/27

3.2.1. Strategic cyber education and training policies

Belgium's[126] Cybersecurity Strategy, published in 2021, considers cybersecurity primarily a driver and enabler of digitalisation. The strategy's target groups are the general population, companies, the public sector, and providers of essential services. The last of these includes actors of key importance to the functioning of society, both in the public and private sectors.

Cybercriminals, foreign security services, terrorist groups and hacktivists are identified as the main threats to cybersecurity. New risks arising from technological development are also highlighted in the strategy. These include the potential vulnerabilities of cloud services or IoT. The lack of human resources is strongly emphasised in the Belgian Cybersecurity Strategy. The inadequacy of experts in the field is described as a threat that must be taken seriously. High-skilled experts are considered the foundation of cybersecurity, whose expertise also helps secure other people's network use. The requirement for experts applies especially to the country's school system, but there is also demand in businesses. RHEA, a cybersecurity company, is establishing[127] an excellence centre employing 300 people in 2023. Belgium plans to spend around 61 million euros from the[128] EU's recovery package on improving cybersecurity.

The strategy sets out six objectives, which will be addressed in particular during the strategy period (2021–2025). These include strengthening the digital environment and increasing trust in it, arming users and service providers against threats, protecting providers of essential services, and responding to cyber threats. The fifth strategic objective is to improve public, private and academic collaboration, while the sixth one is a commitment to international cooperation. As mentioned, citizens are one of the strategy's four main target groups. The starting point for cybersecurity is that everyone bears responsibility for their own devices and applications and the information they contain. The role of the government and the media is to keep citizens informed of threats against them. The Belgian cybersecurity model can be said to assign great responsibility on the citizens. The Centre for Cyber security Belgium (CCB) plays a key role in the strategy's implementation. It is responsible for coordinating and supervising the country's cybersecurity efforts.

3.2.2. The current state of cyber citizen skills education and training

The Centre for Cyber Security Belgium is a key state actor, which also houses the Belgian CERT. The Centre divides cybersecurity into four areas: home, work, school and government. Established in 2014, the Centre operates under the direct authority of the Prime Minister.

The Cyber Security Coalition (CSC) is a cooperation body that promotes cybersecurity and involves both public and private sector actors. The CSC produces, for example, educational materials, guides and reports and organises campaigns promoting cybersecurity. In the CSC's latest annual report, raising awareness and increasing the number of professionals in the field are pinpointed as the key objectives of improving cybersecurity. The CSC also selects the Cyber Security Personality of the Year from a short list of ten cybersecurity influencers. In 2022, Sebastien Deleersnyder, Chief Technology Officer of Toreon,[129] was selected as one of the ten finalists.

The state-run Safeonweb.be website compiles cybersecurity information for citizens. The content of the site is available in four languages: Flemish, French, German and English. In addition to tips and tests, the site offers "first aid" for various cybersecurity-related situations. These guidelines cover various practical situations that are risky in terms of cybersecurity – from spam to extortion, and from losing a smart device to clicking on the wrong link. Users can also forward suspicious emails they receive to the site.

There is need for information and support, as Safeonweb.be receives on average around 12,000 messages from citizens every day.[130] On the other hand, this figure demonstrates the good reach of the service. Around 200,000 people have downloaded the Safeonweb application[131], which alerts them to new cybersecurity threats directly on their mobile phones. Awareness of Safeonweb's annual campaigns is about 55 per cent.

Cybersecurity is already considered part of daily safety. Besafe.be is an information website focusing on safety at home. One of its latest campaigns deals with the risks posed by smart home devices.[132] Risk-info.be, which focuses on preparedness and security, also addresses the basics of cybersecurity. Febelfin, a financial sector federation, provides consumers with information on the safety of online[133] financial transactions. Telecom operators also coordinate[134] action against online scams and actively inform their customers about threats.

The Belgian education system is divided into different systems based on the country's three languages (French, Flemish, German)[135]. The systems are very similar. The education system is also divided according to the schools' background, which can be a linguistic area, an administrative district or another type of community, usually the Catholic Church. In matters related to information technology, schools in practice have the power to decide on the content and methods of teaching. The federal government decides only on the school starting age and, indirectly, on the funding of schools. Because of this division, it is impossible to give even a rough picture of the state of cybersecurity in schools or the content of teaching. It is fair to assume that large differences are found in the teaching of cybersecurity. Further evidence of this comes from the NCSI Cyber Security Index, in which Belgium scores only one point out of two for primary and secondary education[136], compared to 2/2 for all other levels of education and other education-related topics.

Around eight per cent of university students in Belgium are in the ICT sector[137], and the need for cyber professionals in the country is high on the Union scale[138]. University degrees in cybersecurity can be completed at more than 20 universities and universities of applied sciences in the country.[139] Almost all of the degrees are provided by a single institution, but there is also a two-year Master's programme in cybersecurity that is jointly provided by six institutions.[140] The programme is almost entirely in English, but a small part of the teaching is in French. These can also be replaced with courses held in English.

The Click safe website of Child Focus, a child protection organisation, focuses specifically on children's safety online. The organisation's activities focus on the prevention of child abuse and child trafficking. Child Focus is also a key player in the biannual Internet Safe and Fun Day[141], where volunteers trained by the organisation talk to schoolchildren about cybersecurity. Since 2010, the event has reached 93,000 schoolchildren.[142]

According to research, older internet users are more uncertain[143] about their skills than younger users. For this reason, campaigns have been targeted at the older population[144] to guide and encourage them to use the internet.

In 2022, the B-BICO project brought together experts from different fields to discuss the media literacy of vulnerable groups and ways to support it. The report, published in late 2022, makes nine policy recommendations. The first four focus on children, highlighting the accessibility of online services, the importance of digital skills taught in schools, the suitability of teaching materials, and the identification and recognition of the importance of digital mentoring. The other five are for parents. The first deals with the use of plain language, videos and other forms of expression in educational materials. This often helps parents with inadequate language skills. It also highlights the importance of flexibility and diversity in education, improving parents' level of knowledge and skills, raising parents' interest in their children's digital environment and providing tips on how to establish family rules and practices.[145]

Information about online fraud is available in French at traquelarnaque.be [146] and in Flemish at spotdescam.be[147]. The Cyber Security Challenge[148] is a competition for teams of four students launched in 2015, which aims to raise awareness of cyber threats and inspire students to enter the field. The importance of the pan-European competition is underlined by the Belgian final being held at the Royal Military Academy.

3.2.3. National characteristics

Even Belgians themselves consider their government structure complex. The country is also divided by two official languages, Flemish and French. The country's Cybersecurity Strategy[149] mentions this as a factor that makes a coordinated and comprehensive cybersecurity policy difficult. Indeed, the instructions and guidance of the Centre for Cyber Security are only instructions and guidelines, not orders or provisions. As such, security, including cybersecurity, is a federal matter in Belgium.

The fact that Belgium is home to various institutes of international operators, most notably the European Union facilities and the NATO headquarters, adds a further nuance to cybersecurity. The country supports the cybersecurity of these operators, assigning them to the same category as its own essential services.

The Belgian Ministry of Defence was hit by a cyberattack in December 2021. After that, in early 2022, the country committed to spending more than a hundred million euros to improve cybersecurity and capabilities.[150]

3.2.4. The definition of cyber citizen skills

The Belgian Cybersecurity Strategy obliges citizens to take responsibility for the information technology in their possession and for the related applications and information. The required cyber citizen skills are thus defined through responsibility. This can be attributed at least partly to the highly fragmented nature of Belgian society, which does not allow for the implementation of more specific objectives or provisions.

References

[126] Centre for Cybersecurity Belgium, *Cybersecurity Strategy Belgium 2.0 – 2021–2025* (2021).
[127] "RHEA Group Announces New European Cybersecurity Centre of Excellence", *RHEA Group,* accessed on November 25, 2022. https://www.rheagroup.com/rhea-group-announces-new-european-cybersecurity-centre-of-excellence/.
[128] "Belgium to spend millions improving national cyber security", *The Brussels Times*, accessed on January 3, 2023. https://www.brusselstimes.com/203570/belgium-to-spend-millions-improving-national-cyber-security.
[129] Cathy Suykens, "Sebastien Deleersnyder is Belgium's Cyber Security Personality of the Year 2022!", *Cyber Security Coalition.be,* 7 October 2022 blog, https://blog.cybersecuritycoalition.be/sebastien-deleersnyder-is-belgiums-cyber-security-personality-of-the-year-2022/.
[130] "2021: Activity report of the Cyber Security Coalition", *Cyber Security Gazette*, accessed on November 25, 2022. https://annualreport.cybersecuritycoalition.be/nl/annualreportcybersecuritycoalitionbe/.
[131] "Ambitions and achievements in the field of cyber security in Belgium", *Centre for Cyber Security Belgium*, accessed on December 14, 2022. https://ccb.belgium.be/en/news/ambitions-and-achievements-field-cyber-security-belgium.
[132] "Appareils connectés", *ibz*, accessed on November 25, 2022. https://www.besafe.be/fr/vol/appareils-connectes.
[133] "Payer par voie digitale et la banque digitale", Febelfin ,accessed on December 14, 2022. https://www.febelfin.be/fr/themes/payer-par-voie-digitale-et-la-banque-digitale.
[134] Krystina Sferlazza, "What is Proximus doing to counter online and telephone fraud?", *Proximus*, April 28, 2022 blog, https://www.proximus.com/news/2022/20220428-blogpost-ksferlazza-fraud-prevention.html.
[135] "Education Structure in Belgium", *belgiumeducation.info*, accessed on November 25, 2022. https://www.belgiumeducation.info/education-system/education-structure.html.
[136] "Belgium", *NCSI*, accessed on November 25, 2022. https://ncsi.ega.ee/country/be/.
[137] "Distribution of graduates and new entrants by field", *OECD.Stat*, accessed on January 3, 2023. https://stats.oecd.org/Index.aspx?datasetcode=EAG_GRAD_ENTR_FIELD.
[138] Borka Jerman Blažič, "Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?", Education and Information Technologies 27 (2022): 3011–3036, https://doi.org/10.1007/s10639-021-10704-y.
[139] "ICT security education in Belgium", *Centre for Cyber Security Belgium*, accessed on December 14, 2022. https://ccb.belgium.be/en/ict-security-education-belgium.
[140] "Master in Cybersecurity", *Ecole Royale Militaire, Université Libre de Bruxelles, Université Catholique de Louvain, Université de Namur, Haute Ecole de Bruxelles, Haute Ecole Libre de Bruxelles*, accessed on December 20, 2022. https://masterincybersecurity.ulb.ac.be/.
[141] "Internet safe and fun", accessed on December 14, 2022. https://internetsafeandfun.be.
[142] "Internet Safe & Fun Days," *Proximus*, accessed on December 14, 2022. https://www.proximus.com/digital-society/trust/internet-safe-and-fun-child-focus.html.
[143] Karel Vandendriessche, Eva Steenberghs, Ann Matheve, Annabel Georges and Lieven De Mare, *imec.digimeter 2020: Digitale trends in Vlaanderen*, (Belgium: imec, 2020).
[144] "Cybersecurity campaign for elderly people", *DNS Belgium*, accessed on December 14, 2022. https://www.dnsbelgium.be/en/news/cybersecurity-campaign-elderly-people.
[145] "Creating a better internet for all - How to include and support vulnerable groups?", *Belgian Better Internet Consortium (B-BICO), CSEM, Média Animation, Mediawijs*, accessed on December 20, 2022. https://b-bico.be/IMG/pdf/policy_brief_better_internet_for_all_eng.pdf.
[146] "Traque l'Arnaque", accessed on December 14, 2022. https://www.traquelarnaque.be/.
[147] "Spot De Scam", accessed on December 14, 2022. https://www.spotdescam.be/.
[148] "Cyber Security Challenge Belgium", accessed on December 14, 2022. https://www.cybersecuritychallenge.be/.
[149] Centre for Cybersecurity Belgium, *Cybersecurity Strategy Belgium 2.0 – 2021–2025* (2021).
[150] "Belgium to spend millions improving national cyber security", *The Brussels Times*, accessed on December 27, 2022. https://www.brusselstimes.com/203570/belgium-to-spend-millions-improving-national-cyber-security.

3.3. Bulgaria

ITU, Global Cybersecurity Index (GCI) 2020	77/182 (Global), 37/46 (Europe)
National Cyber Security Index (NCSI) 2022	26/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	26/27

3.3.1. Strategic cyber education and training policies

In 2016, the Bulgarian Council of Ministers (Министерски съвет) published the National Cybersecurity Strategy, Cyber Resilient Bulgaria 2020. The strategy, updated in April 2021, has been extended until 2023. One of the main objectives is to raise the awareness, knowledge and skills of all stakeholders, strengthen the cybersecurity culture and create a supportive framework for research and innovation. Cybersecurity and the responsible and safe use of information and communication technologies will be integrated into teaching at all levels of education, and teacher training will be increased. Modern, innovative, inclusive and inspiring methods, such as gamification, are used in teaching and campaigning. Several awareness-raising campaigns are planned with the aim of improving citizens' level of cyber hygiene. Raising cybersecurity awareness is a key objective to make citizens aware of cybersecurity risks and preventive measures.[151,152]

One of the objectives of the Digital Bulgaria 2025 programme is to strengthen cybersecurity capabilities. A key measure is to raise awareness among ICT users of the importance of cybersecurity and secure online behaviour.[153] The Digital Skills Strategy is part of the Digital Transformation 2020–2030 policy. The education system is being reformed to improve the digital skills of the workforce. In 2021, €2 million was budgeted for additional training for teachers and academic staff. A digital learning platform is being designed for the adult population through which free digital skills education can be offered. Bulgaria is investing €2.9 million in 21 training centres across the country. They provide students and young people with free digital skills training, including cybersecurity. Efforts will be made to improve the digital skills of the unemployed, seniors, the disabled and other groups at risk. Citizens are encouraged to use e-services, while cybersecurity training is provided to strengthen trust in e-services. According to the policy, the vulnerabilities of cyberspace, the full potential impact of which are unknown, make it important to develop a culture of cybersecurity for society at large.[154,155]

3.3.2. The current state of cyber citizen skills education and training

The Digital Bulgaria 2025 programme will modernise the teaching of information technology in schools. The measures to be taken include reforms to the curriculum and teaching methods, and additional teacher training.[156] In the Bulgarian education system, the teaching of IT skills begins in the third grade of elementary school with computer modelling studies and continues with IT studies in lower secondary school and in the first grade of upper secondary school. Matters related to safety and security are taught as part of these subjects at all levels. Learning objectives related to safety and security apply to everyone. The content and methods of teaching vary according to the age of the target group.[157,158]

Grades III–IV study the prerequisites for safety and security in the digital environment and grades V–VII study the internet and data protection. Students will learn to follow the guidelines for safe internet use and the code of ethics for electronic communications. Grades VIII–X focus on the impact of digitalisation on health and the environment and how to prevent harmful effects. Grades XI–XII focus on media and information literacy. Critical thinking and media literacy are a cross-curricular, cross-disciplinary theme in Bulgarian schools. The aim is to educate informed and thinking citizens who are able to analyse media communications and operate in media environments. Many schools have developed policies on internet safety and information security. They include

rules on ethical online behaviour and cybersecurity, as well as measures to prevent high-risk online behaviour. The Bulgarian State Agency for Child Protection has issued online safety and security rules for kindergartens and schools, while the Bulgarian Safer Internet Centre (SIC) has issued recommendations for cyber-secure distance learning.[159]

The e-Government Agency (Електронно управление) and the Ministry of Education and Science (Министерството на образованието и науката) have jointly developed a digital cyber hygiene lesson plan and a teacher's guide for schools. Interactive teaching includes cybersecurity information, videos and tests. Parents have their own cyber hygiene module.[160] One of the main tasks of the Bulgarian Ministry of e-Governance (Министерството на електронното управление) is to ensure the safety of children and young people on the internet. The Ministry carries out its mission through various events and initiatives.[161] Many NGOs offer cybersecurity training and materials to different target groups. There are clubs for children and young people that also discuss matters related to cybersecurity. Many universities offer cybersecurity education. For example, the University of National and World Economy, Varna Free University and the National Military University "Vasil Levski" offer Master's degrees in cybersecurity. Companies are also training their employees.[162,163]

The Bulgarian Safer Internet Centre (SIC), established in 2005 by the Applied Research and Communications Fund (ARC Fund), promotes the safe, responsible and positive use of information technologies and the internet. The future of its operations is uncertain due to insufficient funding. The main target groups are children, young people and teachers. The SIC is part of the Insafe, INHOPE and Better Internet for Kids international networks supported by the European Commission. Its advisory board includes about 30 representatives of Bulgarian and international institutions, including ministries. With schools and municipalities, the SIC organises various activities, such as campaigns, workshops and training. In 2021, the SIC trained teachers across the country to improve their students' media literacy. The training was based on the Digital Competence Framework for Citizens (DigComp), which includes safety as one of its components. The SIC's SafeNet website provides practical information about cybersecurity risks. The site offers a variety of manuals, publications, presentations, news and lesson plans. The SIC has its own hotline for reporting illegal and harmful content on the internet, a helpline for cybersecurity issues, and a SafeNet application for mobile devices. Its YouTube channel provides videos on cybersecurity risks that can be used in schools to support teaching. An animated series with six episodes (Кибер сбирка), released in 2021, addresses the main risks on the internet.[164,165]

In 2021, the ARC Fund and the SIC developed and deployed new teaching methods in schools aimed at preventing cybercrime and online abuse and improving children's digital literacy. Around 1,500 children, 200 teachers, 270 parents and 1,160 professionals participated in training and awareness-raising campaigns organised by the ARC Fund and the SIC in 2021. Since 2010, the SIC has had its own youth panel of volunteers aged 14 to 18. The youth panel organised the 2021 Bulgarian Safer Internet Day, which was attended by more than 20,000 people. Since 2015, the SIC has run the Cyberscout training programme with the support of the Ministry of Interior (Министерство на вътрешните работи) and Telenor Bulgaria. The educational programme, which has enjoyed great success in dozens of schools, is aimed at children in the fifth grade. Participants complete a two-day cybersecurity training course. Certified Cyberscout pupils tell their peers how to act responsibly and safely on the internet, give advice on internet-related issues, and arrange cybersecurity events.[166,167]

The mission of the Media Literacy Coalition is to promote media literacy among citizens of all ages. Since 2018, the Coalition has organised annual media literacy days. During the 2021 media literacy day, free one-day cybersecurity workshops were held in three different locations. The Coalition trains mentors who guide other citizens in their own networks. The training covers issues such as fake news, online scams and data protection. More than 200 mentors have been trained across the country. In addition, the Coalition provides tailored training for citizens over 55 years of age who have access to the internet but not yet the necessary skills. Topics covered in the training include the identification of disinformation, propaganda, fake profiles, conspiracy theories and scams.[168,169]

UNICEF Bulgaria helps children and young people develop digital skills and critical thinking to learn how to protect themselves from cyber attacks, cybercrime and online violence, identify fake news and make smart decisions online. In recent years, UNICEF Bulgaria has invested especially in the cybersecurity skills of young people. In 2019, it published the "My Right to an Opinion" guide for young people, discussing social media safety, among other things. In 2020, UNICEF Bulgaria organised a Hackathon where young people had the opportunity to present their own solutions related to media literacy and cybersecurity. Plans are underway for a Cyber Survivor application for young people aged 11 to 14.[170,171]

In 2021, the Bulgarian e-Government Agency organised the National Cybersecurity Month (ECSM) for the fourth time. In addition to common European cybersecurity themes, the campaign includes national themes. The ambassadors of the 2021 campaign were two well-known Bulgarian actors, Aleksandra Sarchadjieva and Kitodar Todorov. During the Cybersecurity Month, they shared campaign messages, infographics and advice on social media, and invited expert guests to discuss cybersecurity issues. Thanks to the celebrity partners, the campaign achieved great visibility and positive feedback from citizens. The videos were shown 30 times a day at all the metro stations in Sofia throughout October. There has been talk in Bulgaria about organising similar campaigns throughout the year, as knowledge and awareness are prerequisites for behavioural change. The campaigns have functional learning as their strategy, which means providing genuine examples, communicating up-to-date information on an ongoing basis and teaching basic terminology and practices.[172] The main theme of the 2022 ECSM was protecting children from cybercrime.[173]

3.3.3. National characteristics

In 2019, the Sofia Security Forum surveyed the cybersecurity skills of Bulgarians aged 11-18. The results indicated that children and young people spend more and more time online. The internet plays an important role in the leisure time of children and young people. The majority of 11-18-year-olds say they are aware of online risks and the related safety and security guidelines. However, many do not follow the guidelines. About 30 per cent of the respondents had been personally exposed or knew someone who had been exposed to cybercrime. More than a quarter of respondents did not know to whom or how to report cybercrime. According to the study, this demonstrates the need for more cybersecurity awareness campaigns and training in Bulgaria. Nearly half of the respondents had not received any training related to cybersecurity. Most of them were aged 17–18. The respondents had received training especially in school, but nearly half of the 17–18-year-olds had learned cybersecurity on their own.[174]

3.3.4. The definition of cyber citizen skills

The Ministry of e-Governance provides citizens with instructions for safe online behaviour. Its website contains material published by Europol, describing how to create a cyber secure home (for example backup, passwords, antivirus), how to shop securely online (for example reliable online shops and the use of credit cards), how to stay alert (for example sharing information, links and attachments) and what cybersecurity means in the case of children (for example security of smart toys).[175] The website of the Ministry of Interior's Cybercrime Unit provides advice to citizens on the following matters: passwords, phishing, personal data, licensed software, antivirus protection, monitoring of financial transactions, updates to operating systems and software, backups, two-step authentication and netiquette.[176] Cyber citizen skills are also defined on the basis of the DigComp framework.

References

[151] Министерски съвет, *Национална стратегия за киберсигурност Киберустойчива България 2020* (2016).
[152] Министерски съвет, *Актуализирана Национална стратегия за киберсигурност КИБЕРУСТОЧИВА БЪЛГАРИЯ 2023* (2021).
[153] "НАЦИОНАЛНА ПРОГРАМА „ЦИФРОВА БЪЛГАРИЯ 2025, ПЪТНА КАРТА ЗА ПЕРИОДА ДО 2025, Отчет към декември 2021г.", accessed on 16 November 2022, https://egov.government.bg/wps/wcm/connect/egov.government.bg-2818/ea3fa5bc-f762-479e-8fcd-472cc8af68da/patna_karta_2021_24jan2022.docx?MOD=AJPERES&CVID=ofQZ43R.
[154] European Commission, *Digital Economy and Society Index (DESI) 2022: Bulgaria* (2022), 6–18.
[155] Council of Ministers, *Digital Transformation of Bulgaria for the Period 2020–2030* (2020), 9.
[156] "National Program "Digital Bulgaria 2025" and Road map for its implementation are adopted by CM Decision №730/05-12-2019", *Republic of Bulgaria, Ministry of Transport and Communications*, accessed on September 1, 2022. https://www.mtc.government.bg/en/category/85/national-program-digital-bulgaria-2025-and-road-map-its-implementation-are-adopted-cm-decision-no73005-12-2019.
[157] A personal communication to the researcher, 31/10/2022.
[158] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10–58.
[159] A personal communication to the researcher, 31/10/2022.
[160] "УЧЕНИЦИТЕ ЩЕ УЧАТ ЗА СИГУРНОСТТА В ИНТЕРНЕТ ОТ ДОГОДИНА", *Republic of Bulgaria, Ministry of Education and Science*, accessed on 16 November 2022, https://web.mon.bg/bg/news/3136.
[161] "МЕУ обучава тийнейджъри как да различават фалшивите новинии в Интернет", *Министерство на електронното управление*, accessed on 16 November 2022, https://egov.government.bg/wps/portal/ministry-meu/press-center/news/learning.hackthefake.
[162] A personal communication to the researcher, 05/10/2022.
[163] A personal communication to the researcher, 30/09/2022.
[164] Bulgarian Safer Internet Centre Safenet.bg, *Public report* (2021), 2–20.
[165] "Safenet.bg", *The Bulgarian Safer Internet Center*, accessed on September 1, 2022. https://www.safenet.bg/en/.
[166] Applied Research and Communications Fund, *Annual Report 2021*, 31–34.
[167] "The Cyberscout Training Programme", *Safenet.bg*, accessed on September 1, 2022. https://www.safenet.bg/en/initiatives/173-cyberscouts.
[168] A personal communication to the researcher, 21/07/2022.
[169] "Media Literacy Coalition", accessed o–n September 1, 2022. https://gramoten.li/home/.
[170] "UNICEF launches digital literacy campaign - 'New generation with critical thinking'", *UNICEF Bulgaria*, accessed on November 2, 2022. https://www.unicef.org/bulgaria/en/unicef-launches-digital-literacy-campaign-new-generation-critical-thinking.
[171] A personal communication to the researcher, 27/10/2022.
[172] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 69–93.
[173] Metodi Yordanov, "Child Protection at Focus of European Cybersecurity Month in October", *BTA*, September 27, 2022. https://www.bta.bg/en/news/bulgaria/334269-child-protection-at-focus-of-european-cybersecurity-month-in-october.
[174] Sofia Security Forum, *Оценка на познанията за сигурността в интернет*, Survey on the Knowledge and Aptitudes of Young People for their Security Online (2019).
[175] "Бъдете виртуални и защитени", *EGOV.BG*, accessed on November 3, 2022. https://egov.bg/wps/portal/egov/kibersigurnost.
[176] "БОРБА С КИБЕРПРЕСТЪПНОСТТА, ГДБОП-МВР", accessed on November 17, 2022. https://www.cybercrime.bg/.

3.4. Spain

ITU, Global Cybersecurity Index (GCI) 2020	4/182 (Global), 3/46 (Europe)
National Cyber Security Index (NCSI) 2022	9/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	7/27

3.4.1. Strategic cyber education and training policies

In terms of cybersecurity, Spain has a unique position in Europe and worldwide, with separate organisations specialising in cybersecurity. [177] The National Cybersecurity Strategy (2019) highlights and encourages cooperation between the private and public sectors through the National Cybersecurity Forum. The Forum's three working groups focus on (1) cybersecurity culture, (2) industry and research, development and innovation, and (3) cybersecurity education.[178] The Cybersecurity Strategy sets out general guidelines for cybersecurity, which is why Spain needs to further strengthen skills to tackle cyber threats. Creating a cybersecurity culture is one of the main themes, and includes raising cybersecurity awareness in society and ensuring the right to operate safely, reliably and responsibly in cyberspace. As cybersecurity is a continuously evolving field, the Spanish cybersecurity industry requires continued support and encouragement. This calls for knowledge and a variety of skills.[179]

A cybersecurity culture and commitment to it must be promoted, while strengthening human and technological skills. A cybersecurity culture will be developed through awareness-raising campaigns targeted at citizens and businesses in which each target group is provided with tailored information, particular attention being paid to individual entrepreneurs and small and medium-sized enterprises. Social responsibility for cybersecurity will be increased, and initiatives and plans to promote cybersecurity and digital literacy are encouraged. Measures will be taken to contribute to truthful and high-quality information where fake news and disinformation stand out. Cybersecurity awareness and education will be increased in schools, where they will be adapted to different levels of education. Cooperation with the media will be increased to ensure greater visibility to citizens' campaigns.[180] A national cybersecurity culture is very important to Spain. Members of society are encouraged to build a culture in which citizens share the responsibility for national cybersecurity.[181] Spain is working hard to improve its cybersecurity culture at all levels. This is done, for example, through various training courses, awareness campaigns and portals dedicated to the topic. The goal is to identify the gaps and "protect" them with new campaigns in line with the prevailing situation in the cyber world. Spain has a great deal of material, websites, guidance and campaigns for different target groups. However, there is always room for improvement, and the 360° approach is the only correct one to improving cybersecurity culture.[182] The motto of INCIBE's strategy for 2021–2025 is "De miles a millones" (From thousands to millions). The effects of INCIBE's measures will be leveraged to reach more and more citizens and businesses, helping to increase their level of cybersecurity. The intention is to position Spain as a leading player internationally and a model European benchmarking country in the field of cybersecurity. The goal is for the level of cybersecurity of the country's citizens and businesses to be among the top five in the world. In addition, INCIBE is to be positioned as an exemplary actor in the field of cybersecurity.[183,184]

3.4.2. The current state of cyber citizen skills education and training

Cybersecurity awareness should be part of education programs to ensure everyone has a set of cybersecurity skills. People at home and in organisations form the first line of defence for cybersecurity and therefore need to be aware of the risks they can face.[185] It is impossible to form a comprehensive and accurate picture of the

current state of cybersecurity culture and the impact of the initiatives implemented. This is due to there being inconsistencies between many of the awareness-raising campaigns and initiatives, as they are neither assessed nor reported on. For example, in addition to the school curricula not including enough cybersecurity content, cybersecurity awareness-raising efforts at schools do not reach their target audience, despite there being a wealth of material available. Some of the important projects and services are unknown to the public.[186]

In Spain, ICT is initially taught as part of other subjects in lower secondary education and later as a separate subject. ICT covers ten different areas, four of which are integrated into other subjects and compulsory to all pupils in lower secondary schools. Safety and security is one of these. Although the learning objectives for ICT have not been nationally defined in primary schools, some autonomous communities use them. In Andalusia, for example, the subject "culture and digital practices" focuses on security.[187] According to ENISA's CyberHEAD database, Spanish universities teach cybersecurity in 23 different programmes.[188]

The Spanish National Cybersecurity Institute INCIBE aims to strengthen digital trust, and improve cybersecurity and resilience. Its activities include research, and service provision and coordination, which contribute to cybersecurity nationally and internationally. INCIBE's target groups are citizens, the academia, the RedIRIS research network, cybersecurity professionals and businesses. Its slogan is "INCIBE es ciberseguridad" ("INCIBE is cybersecurity").[189,190] To create a cybersecurity culture that includes strengthening the digital trust and cybersecurity capabilities of citizens and businesses, it is necessary to invest in awareness of the risks associated with digitalisation and in cybersecurity education. All these activities are developed through INCIBE's channels aimed at different audiences. The campaigns include awareness-raising and informative activities, such as large-scale campaigns for different target groups, events and activities in the autonomous communities, some of which involve gamification, as well as training.[191]

OSI (Oficina de Seguridad del Internauta)[192] is a channel for increasing cybersecurity awareness. Its target group comprises citizens who use the internet without adequate knowledge of information technology, communication and cybersecurity. Various tools are used to raise awareness.[193] The site includes 19 different awareness campaigns, such as the "Experiencia Senior" section for seniors, which offers information, exercises and activities, such as crossword puzzles. The site also includes a comprehensive cybersecurity guide (Guía de ciberseguridad. La ciberseguridad alcance de todos), which is suitable for everyone, even though it is part of the section for seniors. The guide deals with device security, the protection of user accounts and personal data, safe internet use, various types of fraud, and the risk-free use of social media. It also contains a security checklist, links to additional information and instructions for reporting, as well as contact information for the national police. INCIBE has co-authored a book with the national police through OSI.[194] In Spain, cybersecurity is also taught with the help of games. This offers a fun way to learn cybersecurity, for example, with family or friends, using various do-it-yourself board games. ¡Contraseñas seguras!, which must first be assembled, is a game that teaches players to make passwords more secure.[195][196]

Administered by INCIBE, Internet Segura for Kids (IS4K) by the Safer Internet Centre (SIC) is part of the European Union's Better Internet for Kids (BIK) programme and the Insafe and INHOPE networks. The target group comprises children and young people and, through them, parents and other educators.[197,198] In 2021, more than 40,000 people participated in more than 200 IS4K education and awareness-raising events.[199] The programme includes events such as the annual Safer Internet Day.[200] "Cybersecurity in your backpack" is a school start campaign that teaches children to use their device responsibly at school. A campaign with instructions and applications for screen time and content management, among other things, is offered to children's parents.[201] INCIBE has also made educational online and mobile games for children and families. Cyberscouts, an online game aimed at the whole family, teaches safe internet use. It has different levels and separate sections for children and adults. Players learn about good and bad passwords, cybersecurity terminology, safe and unsafe situations, and basic concepts of encryption.[202,203] In the second version of the Hackers vs Cybercrook mobile game, players take the role of Sergio and learn about security in everyday situations.[204]

Companies and professionals have access to MOOC courses and Hackend, a free game dealing with cybersecurity in businesses. The game won the award for "Best Serious Game" at the 2016 Fun & Serious Game Festival.[205,206] Hackend (online/mobile) teaches players about cybersecurity in SMEs. The tasks concern everyday situations in SMEs (such as email use) and situations in which the company's data or resources have been compromised (such as data leakage, social manipulation or malware infection).[207] Companies are also offered sector-specific cybersecurity training.[208] For example, there is a training package for tourism with 29 items, each of which contains additional information and training material.

INTEF, the national institute of educational technology and teacher training, offers e-learning courses, such as #SeguDig, on AprendeINTEF, an education meeting point. The course deals with digital security and privacy, and aims to educate teachers in the safe and responsible use of the internet by minors. Topics addressed include viral challenges, fake news, digital wellbeing and addictive online behaviour. This MOOC was created in collaboration with INCIBE and the Spanish Data Protection Agency (AEPD).[209] INTEF's AseguraTIC website provides educational content, guidance, training courses and other useful resources for educators, families, students, schools and administration.[210]

The #ExploradorINCIBE cybersecurity awareness campaign[211] received the Best Video 2021 EU award. The campaign was aimed at people aged 14–64, but its tone was designed with young people in mind. The campaign focused on ransomware, phishing and deepfake video. The campaign got over 75 million views.[212]

Future actions and expectations for raising awareness (examples): All the courses on different topics could be compiled in a single location and large-scale national awareness-raising campaigns could be organised. Educational games could include digital quizzes, escape room-style games, classic timeless games and virtual reality experiences. Support services could collect frequently asked questions in a single location, create a cybersecurity Wikipedia, or compile libraries of cybersecurity applications and interesting content and resources.[213]

3.4.3. National characteristics

All the autonomous communities in Spain (such as Andalusia [AndalucíaCERT], Catalonia [Agencia de Ciberseguridad de Cataluña], Galicia [CIBER.gal] and Castile-Leon [Cybersecurity Innovation HUB]) develop or support initiatives related to cybersecurity or the promotion of a cybersecurity culture and, since the establishment of CSIRTs, the implementation of various awareness campaigns.

3.4.4. The definition of cyber citizen skills

In INCIBE's 2021–2025 strategy, a citizen is defined as anyone who uses technology and devices. Particular attention is paid to minors, as they are a highly vulnerable group.[214] Cyber citizen skills can be analysed through the Common Digital Competence Framework for Teachers (CDCFT), adapted from the European Digital Competence Framework for Citizens and the European Digital Competence Framework for Educators. The framework is divided into five competence areas and a total of 21 competencies. One of the areas is safety, which includes aspects such as the protection of devices, digital identity, data, health and environmental protection. Topics include passwords, privacy protection and cyberbullying, which are also addressed in awareness campaigns and training.[215]

References

[177] Pedro Sánchez Castejón, President of the government of Spain, *National Cybersecurity Strategy 2019* (2019), 14.
[178] National Cybersecurity Forum, *Global report activities carried out in the first phase*, 6, 10.
[179] Pedro Sánchez Castejón, President of the government of Spain, *National Cybersecurity Strategy 2019* (2019), 29–30.
[180] Pedro Sánchez Castejón, President of the government of Spain, *National Cybersecurity Strategy 2019* (2019), 38, 56–57.
[181] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 131.
[182] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 133.
[183] Gobierno de Espãna, INCIBE, *Plan Estratégico INCIBE 2021-2025 'De miles a millones'* (2021), 4–5.
[184] Gobierno de Espãna, INCIBE, *Plan Anual de Actividad INCIBE 2021*, 5.
[185] Foro Nacional de Ciberseguridad, *Foro Nacional de Ciberseguridad, Motor de la colaboración público-privada* (2021), 31.
[186] Foro Nacional de Ciberseguridad, *Foro Nacional de Ciberseguridad, Motor de la colaboración público-privada* (2021), 40.
[187] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 59–60.
[188] "CYBERHEAD – Cybersecurity Higher Education Database", *ENISA*, accessed on November 15, 2022. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=esp.
[189] "What is INCIBE", *INCIBE*, accessed on November 14, 2022. https://www.incibe.es/en/what-is-incibe.
[190] "Qué es INCIBE", *INCIBE*, accessed on November 14, 2022. https://www.incibe.es/que-es-incibe.
[191] Gobierno de Espãna, *España Digital 2026* (2022), 49.
[192] "OSI, Oficina de Seguridad del Internauta", accessed on November 14, 2022. https://www.osi.es.
[193] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 131.
[194] "Guía de ciberseguridad", *OSI*, accessed on September 22, 2022. https://www.osi.es/es/guia-de-ciberseguridad-la-ciberseguridad-al-alcance-de-todos.
[195] "Juegos mesa", *OSI*, accessed on November 14, 2022. https://www.osi.es/es/juegos-mesa.
[196] "Mejora tus contraseñas",*OSI*, accessed on November 14, 2022. https://www.osi.es/sites/default/files/docs/c3_pdf_rp_mejora_tus_contrasenas.pdf.
[197] "Spanish Safer Internet Centre", accessed on November 17, 2022. https://www.betterinternetforkids.eu/sic/spain.
[198] "Internet Segura for Kids (IS4K)", accessed on November 17, 2022. https://www.is4k.es/.
[199]"Cybersecurity Balance 2021 INCIBE", *INCIBE*, accessed on August 16, 2022. https://www.incibe.es/sites/default/files/paginas/que-hacemos/cybersecurity_balance_2021_incibe.pdf?utm_source=google&utm_medium=web&utm_campaign=cybersecurity_balance_2021&utm_id=Cybersecurity+Balance+2021.
[200] "Día de Internet Segura 2023", *INCIBE*, accessed on November 30, 2022. https://www.incibe.es/sid.
[201] "Internet Segura for Kids (IS4K)", accessed on November 17, 2022. https://www.is4k.es/.
[202] "INCIBE lanza Cyberscouts, un juego online para aprender a hacer un uso más seguro de Internet", *INCIBE*, accessed on 15 July 2022, https://www.incibe.es/sala-prensa/notas-prensa/incibe-lanza-cyberscouts-juego-online-aprender-hacer-uso-mas-seguro.
[203] "Juego Cyberscouts", *is4k*, accessed on November 17, 2022. https://www.is4k.es/de-utilidad/cyberscouts.
[204] "Hackers vs Cybercrook", *OSI*, accessed on November 17, 2022. https://www.osi.es/es/hackers.
[205] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 131.
[206] "Hackend, se acabó el juego",*INCIBE*, accessed on November 15, 2022. https://www.incibe.es/protege-tu-empresa/hackend.
[207] "Hackend: se acabó el juego", *INCIBE*, accessed on July 15, 2022. https://www.incibe.es/protege-tu-empresa/blog/hackend-se-acabo-el-juego.
[208]"Bienvenidos, Selecciona el sector al que pertenece tu empresa", *INCIBE*, accessed on November 30, 2022. https://itinerarios.incibe.es/.
[209] "AprendeINTEF, the education meeting point", *INTEF*, accessed on November 18, 2022. https://enlinea.intef.es/?status=in-progress.
[210] "AseguraTIC", *INTEF*, accessed on November 18, 2022. https://intef.es/aseguratic/.
[211] "Explorador INCIBE", *INCIBE*, accessed on November 30, 2022. https://www.incibe.es/exploradorincibe.
[212] "#ExploradorINCIBE", *ECSM*, accessed on November 17, 2022. https://cybersecuritymonth.eu/countries/spain/exploradorincibe/.
[213] Foro Nacional de Ciberseguridad, *Foro Nacional de Ciberseguridad, Motor de la colaboración público-privada* (2021), 42–42.
[214] Gobierno de Espãna, INCIBE, *Plan Estratégico INCIBE 2021–2025 'De miles a millones'* (2021), 10.
[215] INTEF, *Common Digital Competence Framework for Teachers* (2017).

3.5. Ireland

ITU, Global Cybersecurity Index (GCI) 2020	46/182 (Global), 28/46 (Europe)
National Cyber Security Index (NCSI) 2022	30/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	5/27

3.5.1. Strategic cyber education and training policies

In Ireland, the authorities responsible for cybersecurity include the National Cyber Security Centre (NCSC)[216], an operational arm of the Department of the Environment, Climate and Communications (DECC)[217], and Ireland's Computer Emergency Response Team, IRISS-CERT[218]. Ireland's latest National Cyber Security Strategy covers the period 2019–2024. The Cyber Security Strategy defines 20 indicators forming the basis for cybersecurity development in Ireland. Five of the 20 indicators refer in some way to the development of citizens' cybersecurity capital, above all from a business perspective (higher and further education for the needs of workplaces; attracting talent for the needs of workplaces; finding partnerships to fund cybersecurity research; cooperation between industry and government and higher education specialists and funding for such cooperation; and contacts between research and business to drive practical innovation and research breakthroughs). Ireland's stated vision, according to its Cyber Security Strategy, is a society that enjoys the benefits of digitalisation and is involved in shaping the future of the internet. This is further divided into three sections in the Strategy: protection, development and engagement. Protection refers to both the national infrastructure and the security of citizens; development refers not only to institutions, and the public and private sectors, but also to citizens; and participation refers mainly to international cooperation and the development of an international cyberspace. The strategy specifies seven objectives. One of these addresses cyber citizen skills, the aim being to improve citizens' level of knowledge and skills related to cybersecurity and help ordinary people to better understand these skills through information and training. Election influencing and disinformation are also discussed, as is the threat of identity theft and ransomware. The Strategy's section dealing with training and education for citizens mentions, for example, the development of a cybersecurity campaign for citizens (focusing on themes such as cyber hygiene and social engineering). The strategy also considers the 6,500 cybersecurity professionals working in Ireland (2015) and their responsibilities and potential in guaranteeing national cybersecurity, as well as the cybersecurity sector's employment potential overall in the coming years.[219]

3.5.2. The current state of cyber citizen skills education and training

Digital competence is a cross-cutting theme in primary and secondary education in Ireland, and embedding digital technologies in teaching is part of the curriculum development process. Digital competence is combined with other compulsory subjects and elective areas of learning, such as digital media literacy in primary education. In lower secondary school, pupils can study the elective subject "Digital media literacy" and in secondary school, one of the elective subjects is "Computer science". The DigComp framework's Safety competence area is included in the lower secondary school curriculum[220], and cyber hygiene has been one of the key elements of curriculum development.[221] The National Council for Curriculum and Assessment is a body within the Department of Education that provides support material for the Irish curriculum, such as the "Digital media literacy" course for pupils aged 12-15. The course aims to enhance students' opportunities to use digital technologies, communication tools and the internet creatively, critically and safely. To support teachers and schools, an "Assessment Toolkit" is available online, providing support material for learning, teaching, assessment and reporting.[222] Some private companies also support IT teaching in Irish schools. Cyber school.ie

collaborates with primary and lower secondary schools by providing e-learning courses. One of these is an interactive online course, requiring independent study, which covers all the most important areas of cybersecurity and is suitable for pupils, parents and staff in primary, lower secondary and upper secondary schools.[223] The company Computing at schools organises cyber safety & digital citizenship training for 15–18-year-olds either on Zoom or in person at an educational institution. Cyber safety courses are also available for pupils in grades 2–6.[224] In higher education, cybersecurity education is organised by the University College Dublin in its Master's programme "Forensic Computing and Cybercrime Investigation" [225] and by the Technological University Dublin, which offers the programme "Bachelor of Science (Honours) in Computing in Digital Forensics & Cyber Security"[226]. Cybersecurity training for adults is also provided by people's colleges. At least the People's College for Continuing Education and Training in Dublin has a 12-week practical course for adults called "Computers/phones: protect yourself online by keeping your personal information safe".[227]

In Ireland, the third sector plays an important role in cybersecurity education. CyberSafeKids (formerly *CyberSafeIreland*) is an Irish registered charity dedicated to teaching children, parents and teachers safe and responsible online behaviour. It offers live training or webinars provided via the organisation's portal. The "Cyberacademy" portal contains short videos, materials and assignments related to internet safety for children aged 7–10, parents and teachers.[228] The Cyber Threat Task Force is a not-for-profit cybersecurity community that runs an online training campus for citizens and organisations called the "Cyber Risk Academy." The campus's "Interactive cyber awareness training" is aimed at anyone who is concerned about cybersecurity and wants to change their behaviour to avoid falling victim to cyber attacks.[229] Science Foundation Ireland aims to engage the Irish public in science, technology, engineering and mathematics (STEM). To do so, it offers a wide range of activities for children and families, such as the "Mid-term online workshop in cyber security for children".[230] The National Parents Council Primary (NPC) is an association representing parents of children in primary or early childhood education. The NPC's portal provides access to the "Internet safety" online training session, which aims to teach parents how their children can use the internet more safely and responsibly. [231]

The Webwise – The Irish Internet Safety Awareness Centre, co-funded by the EU, aims to promote young people's independent, efficient and safer internet use through a range of information measures aimed at parents, teachers and young people. The Centre develops and supplies resources to help teachers integrate internet safety topics into their teaching, and provides parents with information, advice and tools to help them support their children's safe online behaviour. The Webwise Youth Advisory Panel raises awareness among young people by developing campaigns to prevent cyberbullying, for example. [232]

Campaigns in Ireland are both national and EU-led. "Be Safe Online" is a government campaign highlighting ways to stay safe online. The campaign portal offers a wide range of resources to support the cybersecurity of all citizens, for example, by helping them protect their personal devices and accounts.[233,234] "Be Media Smart" is a campaign focused on disinformation that has been developed by members of Media Literacy Ireland to help people distinguish between reliable and accurate information and intentionally false or misleading information.[235] In addition to national campaigns, Ireland participates in EU campaigns such as Safer Internet Day[236] and ECSM[237]. Safer Internet Day is supported by events and social media campaigns. In connection with the ECSM campaign, the National Cyber Security Centre (NCSC) has published press releases to launch the campaign and information graphics on the government's "Be Safe Online" website, as well as on its Twitter, Facebook and LinkedIn channels.[238]

Ireland's National Police and Security Service maintains a "Cyber Crime" portal, which provides citizens with detailed information about various cyber threats and concrete measures in case of fraud, for example.[239] The police are also involved in "CheckMyLink", a national service implemented jointly with Cyber Skills and ScamAdviser. The goal is to increase consumers' confidence in the authenticity and safety of websites as regards malware, for example. Users can enter the URL of a website in the service, and the service checks the site's safety.[240]

Games related to cybersecurity are available in the MediaLiteracy Ireland portal. The portal's Training & Development tab[241] allows users to search for information and training material on both media literacy and digital security by topic, age group and desired format. For example, games dealing with disinformation include "Fake news game" as well as "GoViral", which helps protect against false COVID-19 information. "#For You" focuses on the fundamentals of internet algorithms.

What is special about cybersecurity training in Ireland is that churches and active volunteers, such as seniors, also participate in training. The Vodafone Ireland Foundation and its partners organise digital skills courses taught by active pensioners from Active Retirement Ireland, a charity. They offer in-person teaching in a variety of community venues across the country. The purpose is to help seniors safely engage in daily activities online.[242] One example of the Church of Ireland's involvement in training is the online seminar "Cybersecurity for the Bewildered: How to keep your computers safe, your data secure and private information out of sight", which was targeted at priests and citizens of Cork, Cloyne and Ross and was implemented by the bishop of the region and the Business Information Systems degree programme at University College Cork.[243]

3.5.3. National characteristics

In Ireland, there is a digital divide between citizens: some master digital skills and others do not ("the haves and the have-nots"). According to a survey carried out in 2020, 42% of Irish people describe their digital skills as below average.[244] Cybersecurity development is challenged by doubts as to whether information campaigns really change behaviour. Moreover, it is uncertain whether cybersecurity should be promoted through the education system, workplaces or private operators.[245] In Ireland, particular attention is now paid to the shortage of employees in the cyber sector. Citizens are offered a variety of courses and programmes to train for jobs in the sector, even if they have no previous experience in it.[246] For example, Generation: You Employed Inc., in cooperation with Microsoft and Verizon, organises "IT Support with Cyber Security" training for beginners who want obtain qualifications for the cybersecurity industry.[247] CareerEra's courses are designed with industry's needs in mind and offer a pathway to cybersecurity tasks to career changers, for example.[248] The ICT Skillnet CISCO Networking Academy offers free cybersecurity courses for both beginners and advanced users.[249] Fortify Institute also offers courses and a portal with key training companies in Ireland.[250]

3.5.4. The definition of cyber citizen skills

Ireland's Cyber Security Strategy does not provide a detailed definition of cyber citizen skills. However, the DigComp framework's Safety competence area is included in the curriculum for lower secondary school. In other words, the teaching of these skills to citizens is supported by the Irish government.[251]

References

[216] "National Cyber Security Centre NCSC", *NCSC,* accessed on 4 January 2023, https://www.ncsc.gov.ie/.
[217] "Department of the Environment, Climate and Communications", *gov.ie*, accessed on 4 January 2023, https://www.gov.ie/en/organisation/department-of-the-environment-climate-and-communications/.
[218] "About IRISS", *Irish Reporting and Information Security Service*, accessed on 4 January 2023, https://iriss.ie/.
[219] Government of Ireland, *National Cyber Security Strategy 2019–2024* (2019).
[220] European Commission, / EACEA / Eurydice, Informatics education at school in Europe, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45, 118.
[221] ENISA, EGA*, Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 28.
[222] "Digital Media Literacy", *National Council for Curriculum and Assessment,* accessed on December 25, 2022. https://curriculumonline.ie/Junior-cycle/Short-Courses/Digital-Media-Literacy/.
[223] "ABOUT CYBERSCHOOL.IE", *CyberSchool.ie*, accessed on December 14, 2022. https://cyberschool.ie/aboutus/.
[224] "Welcome to Computing At Schools", *Computing At Schools*, accessed on December 25, 2022. https://computingatschools.ie/.
[225] "MSc Forensic Computing and Cybercrime Investigation", *University College Dublin*, accessed on December 13, 2022. https://hub.ucd.ie/usis/!W_HU_MENU.P_PUBLISH?p_tag=PROG&MAJR=T146.
[226] "Digital Forensics and Cyber Security", *Technological University Dublin*, accessed on December 13, 2022. https://www.tudublin.ie/study/undergraduate/courses/computing-dig-forensics-and-cyber-sec-tu863/.
[227] "Course Description", *Courses.ie*, accessed on December 25, 2022. https://www.courses.ie/course/computers-phones-protect-yourself-online-keeping-your-personal-information-safe/#.
[228] "CyberSafeKids: Our Story", *CyberSafeKids*, accessed on December 25, 2022. https://www.cybersafekids.ie/about-us/.
[229] "CYBER RISK ACADEMY", *ICTTF International Cyber Threat Task Force*, accessed on December 25, 2022. https://community.icttf.org/courses.
[230] "Mid-term online workshop in cyber security for children", *Science Foundation Ireland*, accessed on December 14, 2022. https://www.sfi.ie/research-news/news/cyber-security-for-kids/.
[231] "Internet Safety – Online," *National Parents Council*, accessed on December 25, 2022. https://www.npc.ie/training-and-resources/training-we-offer/internet-safety.
[232] "About us", *Webwise*, accessed on December 14, 2022. https://www.webwise.ie/welcome-to-webwise/us/.
[233]ENISA, EGA*, Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 43.
[234] "Be safe online", *Government of Ireland*, accessed on December 13, 2022. https://www.gov.ie/en/campaigns/be-safe-online/.
[235] "We need a vaccine against misinformation*," Media Literacy Ireland*, accessed on December 15, 2022. https://www.bemediasmart.ie/.
[236] "Irish Safer Internet Centre – Webwise Ireland", *European Schoolnet*, accessed on December 25, 2022. https://www.saferinternetday.org/in-your-country/ireland.
[237] "Cybersecurity Resources", *ENISA*, accessed on December 25, 2022. https://cybersecuritymonth.eu/countries/ireland.
[238] ENISA, *European Cybersecurity Month (ECSM) 2020 Deployment Report* (2021), 51.
[239] "Cyber crime",*An Garda Síochána (AGS), Ireland's national police and security service*, accessed on December 14, 2022. https://www.garda.ie/en/crime/cyber-crime/cyber-crime-awareness-campaign-2022.html.
[240] "Cyber Skills Ireland launches new service for consumers to support safer online shopping", *CyberSkills Ireland*, accessed on December 25, 2022. https://www.cyberskills.ie/explore/news/name-13692-en.html.
[241] "Training & Development", *Media Literacy Ireland*, accessed on December 25, 2022. https://www.medialiteracyireland.ie/training-development/.
[242] "Digital skills training classes for over 65-year-olds launched | Vodafone Ireland", *Vodafone Ireland Limited*, accessed on December 25, 2022. https://n.vodafone.ie/aboutus/press/multi-million-euro-digital-skills-programme-for-older-people-lau.html.
[243] "Cybersecurity training session in Cork, Cloyne and Ross attracts a lot of interest", *Church of Ireland*, accessed on December 25, 2022. Cybersecurity training session in Cork, Cloyne and Ross attracts a lot of interest - Church of Ireland - A Member of the Anglican Communion.
[244] Accenture, *BRIDGING THE GAP: Ireland's Digital Divide* (2020), 9, 15.
[245]ENISA, EGA*, Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 43.
[246] Carmel Somers and Eoin Byrne, *Cyber security skills report 2021: National survey* (2021), 11.
[247] "IT Support and Cyber Security", *Generation: You Employed Inc.*, accessed on December 14, 2022. https://ireland.generation.org/programs/it-support-2/.
[248] "Cyber Security Course Online", *Careerera*, accessed on December 14, 2022. https://www.careerera.com/cyber-security.
[249] "ICT Skillnet CISCO Networking Academy", *Technology Ireland ICT Skillnet,* accessed on December 15, 2022. https://www.ictskillnet.ie/training/ict-skillnet-cisco-networking-academy/.
[250] "Cybersecurity Training and Education in Ireland – Where do I start?", *Fortify Institute,* accessed on December 14, 2022. https://www.fortifyinstitute.com/blogs/cybersecurity-training?hsLang=en.
[251]European Commission, / EACEA / Eurydice, Informatics education at school in Europe, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45.

3.6. Italy

ITU, Global Cybersecurity Index (GCI) 2020	20/182 (Global), 13/46 (Europe)
National Cyber Security Index (NCSI) 2022	21/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	18/27

3.6.1. Strategic cyber education and training policies

In May 2022, the Italian National Cybersecurity Agency (ACN) published the new Italian Cybersecurity Strategy for 2022–2026 and its Implementation Plan. The Cybersecurity Strategy has three fundamental goals: protection, response and development. They are supported by three enabling factors – cybersecurity training, the promotion of a cybersecurity culture, and cooperation.[252] One of the main objectives of the Strategy is to improve cybersecurity awareness in society at large. Various measures have been prepared to achieve this goal.[253] Cybersecurity education will be enhanced at different levels of education, including comprehensive schools, upper secondary schools, universities and further education programmes. An ACN e-Academy learning platform will be made available to citizens. First, an online tool will be introduced to allow citizens to test their own cybersecurity competence and earn a certificate. Public and private sector employees will be offered more cybersecurity courses and training programmes. To promote a culture of cybersecurity, campaigns will be launched on the risks related to the use of information and communication technologies and on ways to protect privacy online. These campaigns will address the special needs of seniors, people with disabilities and other groups. An independent national strategy and implementation plan will be drawn up for protecting children from cybercrime. It will include campaigns targeting minors and their parents, guardians and teachers.[254]

The goal of the National Digital Skills Strategy (Strategia Nazionale per le Competenze Digitali), published in 2020, and the accompanying implementation plan, is for 70 per cent of Italian citizens to have at least basic digital skills by 2025. The Repubblica Digitale project plays an important role in this. It states that citizens are responsible for operating consciously, safely and sustainably in the digital ecosystem.[255] In 2021, the project had more than 260 different initiatives involving more than 2 million students, 90,000 teachers, 240,000 employees and 1.6 million other citizens. A fund set up in January 2022 will invest 350 million euros in improving the digital skills of 2 million citizens between 2022 and 2026.[256]

3.6.2. The current state of cyber citizen skills education and training

The Italian National Cybersecurity Agency (ACN) was established in August 2021. It is responsible for coordinating the objectives related to education and campaigns outlined in the Cybersecurity Strategy. The Agency aims to develop a systematic approach to cybersecurity education by first mapping the training and education opportunities currently available and then coordinating them. There are a number of public and private actors providing cybersecurity-related education and training in Italy.[257] Information technology, which includes the teaching of digital skills and cybersecurity skills, is taught in varying degrees in basic education as part of other subjects. In secondary education, information technology is a compulsory and separate subject for some pupils and compulsory for all as part of mathematics.[258] According to ENISA's CyberHEAD database, Italian higher education institutions offer a total of 17 degree programmes in cybersecurity.[259] The ACN and the Lazio Region have recently signed a four-year agreement on the provision of cybersecurity training programmes. The training programmes are aimed at secondary schools, higher education institutions and continuing education. Italian IT companies are involved in the cooperation. Training will take place in a new cybersecurity training centre. The project aims to strengthen the security of all of Italy.[260,261]

Italy's Postal and Communications Police (Polizia Postale e delle Comunicazioni) is a special unit that monitors the security of the Italian communications network, prevents cybercrime and ensures the confidentiality of citizens' correspondence and freedom of communication. It promotes cybersecurity awareness among Italian schools, reaching around 500,000 schoolchildren each year in this way.[262] Citizens can use the Commissariato di P.S. Online website and social media channels to request help with cybersecurity issues and report them from home. The website publishes cybersecurity-related news, alerts, tips and information for citizens.[263]

The Italian Safer Internet Centre (SIC), Generazioni Connesse, is part of the Insafe, INHOPE and Better Internet for Kids networks supported by the European Commission. Its operations are coordinated by the Italian Ministry of Education (Ministero dell'Istruzione). The cooperation includes, among others, the Italian police and universities. Generazioni Connesse provides support and information to children, young people, parents, teachers and educators on issues related to the internet and the problems it causes. It has developed an educational package called Kit Didattico for schools, the aim of which is to provide pupils with digital civic skills. The educational package is based on the Digital Competence Framework for Citizens (DigComp), which includes safety as one of its competence areas. Generazioni Connesse's website and social media channels contain news and information about cybersecurity, including malware, phishing, and privacy. The SuperErrori videos and tutorials feature seven online superheroes whose blunders and mistakes teach children and teenagers how to stay safe online.[264]

In 2014, the CINI cybersecurity laboratory (Consorzio Interuniversitario Nazionale per l'Informatica) and the Italian Ministry of Education launched Programma il Futuro, a training project. The project's aim is to provide schools with simple, efficient and easy-to-use tools that help students familiarise themselves with the basic scientific principles of digital technologies and learn how to use digital technologies responsibly. The material also includes cybersecurity. The project's main target groups are schoolchildren and teachers, but the materials are also suitable for use by other citizens. They have been used, for example, in adult education centres and in self-study courses for seniors. Teachers from Italian schools are invited to take part in the project at the beginning of each school year. Participation is voluntary for schools. The teachers' manuals include lesson plans, teaching content and exercises. A website has been created as support for the written materials. Video material is also available for each lesson[265,266]

Ludoteca del Registro.it is a project carried out by Registro.it (the administrator of the .it domain names), the goal being to teach children and young people how to use the internet responsibly. The focus is on cybersecurity. So far, the project has reached around 500 school classes and 14,000 pupils across Italy. Ludoteca del Registro.it is aimed at schoolchildren of all ages. Information and materials are also available for parents and teachers. Teaching is typically organised in workshops, which have cybersecurity as their main theme but also discuss the internet's technical infrastructure. The teaching methods vary according to the age of the target group. Internetopoli is a web application aimed at children in primary school, while the video game Nabbovaldo e il ricatto dal cyberspazio (Nabbovaldo and blackmail from cyberspace) and the related educational path caters to children in lower secondary school and Cybersecurity4Teens to children and adolescents aged 11–19. The Presente Digitale portal is intended for teachers. The materials are free and available to everyone.[267]

Launched in 2009 by Emilia-Romagna local government, Pane e Internet (PEI, Bread and Internet) is an example of a regional training project. Teaching is based on the DigComp framework. The aim of the project is to teach Emilia-Romagna's residents digital skills starting with the foundations and progressing to more advanced levels. The project primarily targets citizens who use the internet less than others, such as the unemployed and housewives, as well as citizens who use the internet but who do not have adequate information security and critical media literacy skills, such as young people. Topics related to cybersecurity include device security, antivirus, passwords and scams. Over the past five years, more than 30,000 citizens have participated in training through the project. Teaching is free for residents of the Emilia-Romagna region. PEI also organises various workshops, conferences and events to promote the safe use of digital technologies.[268,269]

Cybercity Chronicles is a learning game developed jointly by Dipartimento delle Informazioni per la Sicurezza (Security Intelligence Department, DIS) and the Ministry of Education. The aim of the game is to teach especially young people how to use the internet, social media and new technologies responsibly and positively. The action-adventure game is set in 2088 in a sophisticated cyber city, where the wonders of the digital revolution have also introduced various risks. The game includes a Cyberbook glossary with explanations of key cybersecurity concepts.[270,271] Digitalscape, developed by Idea.lab and the regional education group of Lombardy, is a game that develops digital security skills. It is suitable for both in-person and distance education in schools. The games come in two versions: the easier one has 15 parts and is aimed at pupils aged 13 to 14, while the harder one has 21 parts and is aimed at 15–18-year-olds. The game takes the form of a virtual escape room. The topics covered include phishing, spam, digital identity, secure password policies, device security, cyberbullying, and fake news. At present, around 900 teachers use the game in their teaching.[272,273]

CyberHighSchools is a network of schools coordinated by CINI that promotes cybersecurity competence and collaboration among young Italians. Schools can participate in theCyberChallenge.IT training programme and in information security OliCyber.ITOlympics. Participation is voluntary and free.[274] CyberChallenge.IT is a training programme for young people aged 16 to 24, which aims to find future cybersecurity professionals. In 2022, the goal was to attract at least 5,000 students to sign up for the programme. The training programme employs both traditional teaching methods and gamification. The members of the Italian team for the annual European Cyber Security Challenge organised by ENISA are selected through qualifying rounds from the CyberChallenge.IT training programme.[275] CyberTrials is a free game and training programme aimed at Italian girls in upper secondary school. It promotes the themes of information security and digital citizenship.[276] OliCyber.IT, CyberChallenge.IT and CyberTrials jointly form the Big Game at the Laboratory, a project in which university experts and leading companies in the field train young people to become experts in cybersecurity.[277]

The cybersecurity campaign I Navigati - Informati e Sicuri (The cyber aware family – informed and safe), jointly run by public authorities and the finance sector, was launched in 2021. The campaign encourages a safer and more informed use of digital channels and tools, and raises awareness of the risks of cyber attacks and fraud in financial services. The campaign, which addresses all citizens, makes use of television, radio, social media, newspapers and the campaign's own website. It also includes an eight-part miniseries, interviews and information packages. The campaign was renewed for the European Cybersecurity Month 2022.[278]

3.6.3. National characteristics

Italy faces similar cyber challenges as the rest of Europe. In general, citizens' cybersecurity skills need to be improved. Gender and intergenerational gaps should be reduced. More cybersecurity training is required for different levels: there are many higher education degrees, but fewer short cybersecurity courses.[279]

3.6.4. The definition of cyber citizen skills

The definition of cyber citizen skills has been discussed, but no official decisions have been made as of yet.[280] Cyber citizen skills have been defined, for example, on the basis of the DigComp framework. Agenzia per l'Italia Digitale has released DigComp 2.1 in Italian.[281] The general objective is for citizens to understand the basic principles of protecting their personal data and devices, be aware of the different security measures, know how to address reliability and privacy in accordance with the GDPR, and take care of their physical and mental wellbeing.[282]

References

[252] ACN, *National Cybersecurity Strategy 2022–2026* (2022).
[253] A personal communication to the researcher, 25/10/2022.
[254] ACN, *Implementation Plan, National Cybersecurity Strategy 2022–2026(* 2022).
[255] "Il manifesto per la Repubblica Digitale", *Repubblica Digitale*, accessed on October 21, 2022. https://repubblicadigitale.innovazione.gov.it/it/il-manifesto/.
[256] European Commission, *Digital Economy and Society Index (DESI) 2022: Italy* (2022), 7–8.
[257] A personal communication to the researcher, 25/10/2022.
[258] European Commission, / EACEA / Eurydice, Informatics education at school in Europe, Eurydice report (Luxembourg: Publications Office of the European Union, 2022).
[259] "CYBERHEAD - Cybersecurity Higher Education Database," *ENISA*, accessed on 21/10/2022, https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/.
[260] A personal communication to the researcher, 14/06/2022.
[261] "Cybersicurezza: nel Lazio una scuola per professionisti esperti", *Regione Lazio*, accessed on November 14, 2022. https://www.regione.lazio.it/notizie/cybersicurezza-nel-lazio-una-scuola-per-professionisti-esperti.
[262] A personal communication to the researcher, 25/10/2022.
[263] "Commissariato di P.S. online", *Polizia Postale e delle Comunicazioni*, accessed on October 24, 2022. https://www.commissariatodips.it/index.html.
[264] "Generazioni Connesse", accessed on October 24, 2022. https://www.generazioniconnesse.it/site/it/home-page/.
[265] "Programma il Futuro", accessed on October 21, 2022. https://programmailfuturo.it/.
[266] A personal communication to the researcher, 24/05/2022.
[267] Giorgia Bassi, Stefania Fabbri ja Anna Vaccarelli, "Ludoteca del Registro.it: Cybersecurity in Education", *Ercim News,* no. 129, April 2022, 39-40.
[268] "PEI pane e internet", accessed on September 21, 2022. https://www.paneeinternet.it/public/pei-en.
[269] A personal communication to the researcher, 08/07/2022.
[270] "Cybercity: arriva il primo videogioco ambientato nel cyberspazio", *Sistema di informazione per la sicurezza della Repubblica*, accessed on 24 October 2022, https://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/cybercity-arriva-il-primo-videogioco-ambientato-nel-cyberspazio.html.
[271] A personal communication to the researcher, 14/06/2022.
[272] A personal communication to the researcher, 12/07/2022.
[273] "Digitalscape", accessed on November 14, 2022. https://www.digitalscape.it/.
[274] "Cyber High Schools", *cini*, accessed on October 24, 2022. https://cybersecnatlab.it/cyber-high-schools/?lang=en.
[275] "CyberChallenge.IT", *cini,* accessed on October 24, 2022. https://cyberchallenge.it/.
[276] "CYBER TRIALS", *cini,* accessed on October 24, 2022. https://www.cybertrials.it/.
[277] "17 Oct Aperte le iscrizioni di OliCyber e CyberTrials: riparte il grande gioco degli hacker etici", *cini*, accessed on 26 October 2022, https://cybersecnatlab.it/aperte-iscrizioni-olicyber-cybertrials-riparte-il-grande-gioco-degli-hacker-etici/.
[278] "I NAVIGATI, INFORMATI E SICURI", *CERTFin*, accessed on October 24, 2022. https://inavigati.certfin.it/.
[279] A personal communication to the researcher, 25/10/2022.
[280] A personal communication to the researcher, 25/10/2022.
[281] Stephanie Carretero, Riina Vuorikari and Yves Puni, *DigComp 2.1 Il quadro di riferimento per le competenze digitali dei cittadini*, AGID Agenzia per l'Italia Digitale (2017).
[282] AGID Agenzia per l'Italia Digitale, *Competenze digitali per i cittadini: proposte operative*, 11.

3.7. Austria

ITU, Global Cybersecurity Index (GCI) 2020	29/182 (Global), 17/46 (Europe)
National Cyber Security Index (NCSI) 2022	32/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	10/27

3.7.1. Strategic cyber education and training policies

The most recent Austrian Cybersecurity Strategy (ÖSCS ¶ SCS 2021) was adopted in 2021, while the previous one dated back to 2013. The strategy is described as being part of the EU's concerted efforts to improve cybersecurity. It takes as its starting point the rapid digitalisation of all areas of life, the flip side of which is that huge opportunities come with big threats. In accordance with the strategy, these threats must be addressed systematically and flexibly. At the strategic level, cybersecurity is a federally regulated and managed activity. The Cyberstrategy was drafted by the Federal Chancellery and it is implemented by the Federal Ministry of the Interior. The strategy is divided into two parts, the actual strategy and a more concrete implementation plan. The goal of this division is to ensure the ability to quickly react to changing situations. Nevertheless, the country's federal structure means that national measures in the field of cybersecurity, including in schools, are inevitably variable. The federal states have autonomy over their education strategies, which makes it impossible to implement national initiatives and difficult to follow local initiatives.[283,284]

Cybersecurity threats fall into four categories: intentional and unintentional misuse, dependence on information systems, and new threats arising from technological development. Citizens' cybersecurity skills are not included in this categorisation. Instead, the strategy outlines security primarily through organisations. The same applies to the strategy's objectives: the only objective that even remotely refers to citizens is that all parties take responsibility for cybersecurity. On the other hand, one of the objectives is to ensure that all Austrians have a secure platform for taking part in social and political life in cyberspace.[285]

The strategy's target audiences include society at large, business, the education sector and research and development. Citizens' cybersecurity skills belong to the first of these, more specifically under the topic of "awareness". In this context, the strategy underlines that a self-determined and responsible behaviour in cyberspace will help make Austrian society more resilient to cyberattacks. Concerning education, the strategy states that the ever-changing field requires lifelong learning in matters related to digitalisation. Responsibility for the strategy's implementation is assigned to ministries in their respective areas of responsibility. A review is carried out once every six months, in addition to which new concrete milestones are defined for the strategy's implementation. The work is steered by the Cyber Security Steering Group's Secretariat.[286]

Digital competence and media literacy are also key elements in Austria's Youth Strategy.[287] It places particular emphasis on the ability to critically examine the information provided. Every year, the Federal Chancellery publishes a cybersecurity report, which reviews the past year both by administrative branch and from an international perspective. [288]

3.7.2. The current state of cyber citizen skills education and training

In 2022, Digitale Grundbildung (basics of digitalisation), became a compulsory subject in secondary education. It will gradually be expanded to other levels of education and to support it, continuing education has been launched for teachers and plans are to include the new subject in teacher training. Overall, cybersecurity has become an integral part of pedagogical education in Austria. In comprehensive school, the focus of digital skills

is on media education and the reflective use of the internet. In lower grades, a playful approach to technology and problem solving is essential. [289] Various projects related to developing the digital skills of primary school pupils are included in the curriculum under the heading "Thinking, learning and problem solving". Pupils in lower secondary school (grades 5–8) have at least one hour of digital basic education per week. [290] Various parties have collaboratively produced teaching materials and content for the subject. The government, the Austrian Red Cross and the Buch Club, which promotes reading among schoolchildren, have jointly published material suitable for pupils of different ages under the names CyberSPACE and CyberSPOT. [291]

In the general plan of the Austrian Ministry of Education concerning the digitalisation of schools, development activities are divided into content, equipment and teacher competence. The different dimensions of cybersecurity – behaviour and cyber threats – are included in the content, even though they are more closely related to the development of structures, practices and content. [292]

The Cyber Security Platform (CSP) acts as a cooperation body for public and private cybersecurity actors. Among other things, its working groups formulate recommendations for safe internet use. It also contributes to the publication of the annual cybersecurity report. The report reviews the phenomena and events that have influenced cybersecurity during the year, both at home and abroad. [293]

The Vienna Cybersecurity and Privacy Research Cluster (ViSP) is currently cooperating with its partners (the Learners programme, the Austrian Computer Society, Saferinternet.at and Teach for Austria) to produce a plan for teaching Austrian children and young people about cybersecurity through games. After the design phase, the goal is to create online games and challenges.[294]

Founded in 2013, the Onlinesicherheit website provides a wealth of cybersecurity information to meet the needs of citizens, including educational videos, links to software for increased security and up-to-date alerts. The site is run by state actors, but more than 40 partners are involved. The site has different target groups ranging from citizens of all ages to businesses. The site provides citizens with cybersecurity news, security alerts, publications and links to various security programs. It also provides access to webinars on various topics related to cybersecurity. [295]

In PenQuest, a game built jointly by Saint Pölten University of Applied Sciences and the University of Vienna, two players face each other, one as the attacker and the other as the defender. The game's realism builds on the MITRE ATT&CK knowledge base used for attacks, the MITRE D3FEND knowledge base used for defensive action, as well as on the NIST SP 800-53 security standard. [296] The Austrian Chamber of Commerce organises an annual eDay event to promote the digitalisation of Austrian businesses. Cybersecurity is a prominent part of the event. [297]

A new Institute of Digital Sciences Austria (IDSA), which is intended to serve as a catalyst for the country's digitalisation, is being established in Linz. The academic concept of the new multidisciplinary university, which will begin operating in the second half of 2023, includes cybersecurity as part of the basic studies common to all. The goal is to have 5,000 students by the end of the decade and about 150 professors in the mid-2030s. [298]

Higher education in cybersecurity is also available in more than ten institutions in Austria. Some of the programmes are provided in English.[299] Based on scientific references, universities in large cities are at the forefront of this group.[300] Security was the theme of the Austrian Computer Association's magazine 4/22. The content of the professional magazine highlighted the importance of certificates as a means of raising the level of safety and security. [301]

The digitalisation of central government also requires the provision of comprehensive cybersecurity training to officials. For example, the Ministry of the Interior trains around 40,000 police officers and other officials subject to its authority in its own e-Campus learning environment.[302] The police have their own cybercrime competence centre, which offers advice and instructions to citizens. Crimes must nevertheless be reported to a regular police station.[303]

In Austria, the Federal Chancellery sees to the European Cybersecurity Month, coordinating the annual campaign with the aid of guidance and materials produced by ENISA. In cooperation with the Federal Ministry of the Interior and the Federal Ministry of Defence, the Federal Chancellery also organises the Austria Cybersecurity Challenge (ACSC), a competition offering talented young people and IT professionals the opportunity to demonstrate their skills and expertise. The competition also brings visibility to cybersecurity issues. The target group comprises young people aged 14–25.[304,305]

The Österreichische Institut für angewandte Telekommunikation (ÖIAT) is a non-profit organisation that promotes digitalisation through projects. Many of its projects have focused on the different dimensions of citizens' cybersecurity.[306]

Among other things, the ÖIAT has developed a quality label for Austrian online shops, provided information about the early detection of online fraud and developed cybersecurity content for the older population. The malzwei.at website created by the ÖIAT focuses on fake online stores and other scams. Its approach to promoting citizens' cybersecurity has focused heavily on problems associated with online commerce. The ÖIAT boosts consumers' ability to identify potential security threats, and its operations help create an increased sense of security required for digitalisation.[307]

The ÖIAT's Fake Off campaign was aimed at young people, the aim being to improve media literacy. In addition to a website and written material, the campaign included a mobile application, which allowed users to practice source criticism and learn to identify disinformation.[308]

A similar concept promoting digitalisation has been adopted by the fit4internet association, which states as its objective to promote digital skills in Austria.[309] The association's website offers tests in different competence areas, one of which is safety.[310] Tests are available for different levels of users.

The Saferinternet.at website contains information about safe internet use for different target groups. The content is arranged for different target groups: teachers, parents, young people and those working with young people. The site includes, among other things, a quiz-like game related to cyberbullying, as well as comics for young people, coaching for parents, and networking and discussion opportunities for those working with young people.[311]

3.7.3. National characteristics

Austria's digitalisation strategies show a strong emphasis on state measures (legislation and organisation) and the importance of experts. Citizens' knowledge and skills are not discussed much, even though their importance as a key factor in resilience is recognised. For example, the training of cybersecurity professionals is considered more important than raising the competence level of citizens across the board.

3.7.4. The definition of cyber citizen skills

As a rule, Austrian datasets refer to cyber citizen skills at a very general level. Citizens' ability and willingness to operate in a virtual world is primarily considered a competitive factor for the country's economy and the administration's efficiency. [312] While the education and training programmes of various actors are more concrete, the underlying ideas about the necessary cyber citizen skills are not explained in any greater detail. However, school education is based on the DigComp framework.[313]

References

[283] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022), 25.
[284] ÖSCS, *Austrian Strategy for Cybersecurity 2021* (2021).
[285] ÖSCS, *Austrian Strategy for Cybersecurity 2021* (2021).
[286] ÖSCS, *Austrian Strategy for Cybersecurity 2021* (2021).
[287] "Austrian Youth Strategy", *The Federal Ministry of Education, Science and Research*, accessed on November 25, 2022. https://www.bmbwf.gv.at/en/Topics/youth_strategy.html.
[288] "Cybersecurity Report", *Federal Chancellery of Republic of Austria,* accessed on January 4, 2023. https://www.bundeskanzleramt.gv.at/en/topics/cybersecurity/cybersecurity-report.html.
[289] "Digitale Grundbildung", *Bundesministerium*, accessed on November 25, 2022. https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/dgb.html.
[290] "Denken lernen, Probleme lösen – Digitale Grundbildung in der Primarstufe und der Sekundarstufe I", *Bundesministerium*, accessed on 14 December 2022, https://www.bmbwf.gv.at/Themen/schule/zrp/dibi/dgb/dlpl.html.
[291] "Mehr als nur Lesen", *Gemeinsam lesen*, accessed on December 14, 2022. https://www.gemeinsamlesen.at/sekundarstufe.
[292] "8-Point Plan for Digital Learning", *The Federal Ministry of Education, Science and Research*, accessed on November 25, 2022. https://www.bmbwf.gv.at/en/Topics/school/krp/8_p_p.html.
[293] "Nationale Cybersicherheitsstrukturen", *Bundeskanzleramt*, accessed on December 14, 2022. https://www.bundeskanzleramt.gv.at/themen/cybersicherheit/nationale-strukturen.html.
[294] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022).
[295] "Onlinesicherheit", accessed on December 14, 2022. https://www.onlinesicherheit.gv.at/.
[296] "PenQuest", accessed on January 4, 2023. https://www.pen.quest/.
[297] "E-Day", *WKO*, accessed on December 14, 2022. https://www.wko.at/Content.Node/kampagnen/E-Day/index.html.
[298] "Institute of Digital Sciences Austria (IDSA)", *Austrian Federal Ministry of Education, Science and Research: Institute of Digital Sciences*, accessed on December 14, 2022. https://www.bmbwf.gv.at/en/Topics/Higher-education---universities/Institute-of-Digital-Sciences-Austria-(IDSA)-%E2%80%93-A-new%2C-innovative-University-of-Technology-for-Digitalisation-and-Digital-Transformation-in-Austria.html.
[299] "Top – Security University's / Applied Siences / Security Research in Austria", *Cyber Security Austria*, accessed on 20 December 2022, https://verbotengut.at/center-of-excellence/top-security-studies-in-austria/.
[300] "7 Best universities for Cyber Security in Austria", *EduRank*, accessed on 20 December 2022, https://edurank.org/cs/cybersecurity/at/.
[301] Die Österreichische Computer Gesellschaft (OCG), *OCG Journal* (4/22), https://www.ocg.at/sites/ocg.at/files/medien/pdfs/OJ2022-04.pdf.
[302] "eCampus", accessed on 14 December 2022, https://e-campus.st/moodle/.
[303] "Delikte & Ermittlungen", *Bundesministerium*, accessed on December 14, 2022. https://bundeskriminalamt.at/306/start.aspx.
[304] "Cybersecurity Activities and Iniatives", *Federal Chancellery Republic of Austria*, accessed on 27 December 2022, https://www.bundeskanzleramt.gv.at/en/topics/cybersecurity/activities-and-initiatives.html.
[305] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022), 7-8.
[306] "Kompetenz für die digitale Welt", *ÖIAT*, accessed on December 14, 2022. https://www.oiat.at/.
[307] "Malzwei," accessed on December 14, 2022. https://www.malzwei.at/.
[308] "Fake Off", accessed on December 20, 2022. https://www.fake-off.eu/fake-off/.
[309] "Fit4internet", accessed on December 14, 2022. https://www.fit4internet.at/view/verein.
[310] "Safety", *Fit4internet*, accessed on December 14, 2022. https://www.fit4internet.at/page/assessment/sicherheit.
[311] "Saferinternet.at", accessed on December 27, 2022. https://www.saferinternet.at/.
[312] Republic of Austria, *Digitalisation Report #1: NOW FOR TOMORROW Digitalisation for growth and futureproofing* (2021).
[313] "Digi.komp", *Bundesministerium*, accessed on December 20, 2022. https://digikomp.at/.

3.8. Greece

ITU, Global Cybersecurity Index (GCI) 2020	28/182 (Global), 16/46 (Europe)
National Cyber Security Index (NCSI) 2022	1/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	25/27

3.8.1. Strategic cyber education and training policies

In 2020, the National Cybersecurity Authority (NCSA), operating under the Ministry of Digital Governance (ΥπουργείοΘηφιακής Διακυβέρνησης), published the National Cyber Security Strategy for 2020–2025. It lays out a vision of a modern and secure digital environment with information and network infrastructures, applications and services that contributes to economic and social wellbeing and protects the fundamental rights of citizens. A culture of the safe use of digital services and applications will be developed and citizens' trust in digital technologies will be strengthened. One of the main strategic objectives is to build capacities, increase knowledge and raise awareness. This includes the continuous and systematic development of citizens' cybersecurity awareness and skills. A key measure is to draw up an action plan for education and awareness. The cybersecurity strategy proposes a jointly developed national cybersecurity awareness programme that addresses all age and social groups and uses updated information and materials. The aim is to create a cyber hygiene framework and a national culture of cybersecurity awareness.[314]

In 2021, the Digital Transformation Strategy 2020–2025 for Greece and the operational programme for its implementation in 2021–2027 were published. The strategy places great emphasis on the country's citizens. Improving citizens' digital skills is one of the cornerstones of Greece's Digital Transformation Strategy. This includes measures such as increasing the number of weekly IT lessons in primary schools, providing digital skills courses in higher education institutions, strengthening the digital skills of employees, and providing an online digital skills training platform for citizens. The strategy also takes into account different groups at risk, such as people with disabilities and seniors, as well as groups that typically face more challenges in entering the labour market, such as women and the unemployed.[315,316]

3.8.2. The current state of cyber citizen skills education and training

No operator in Greece currently holds overall responsibility for citizens' cybersecurity expertise. Instead, the responsibility is shared between several agencies and ministries. Indeed, coordination is one of the biggest challenges. Problems may arise if roles and duties overlap and several organisations provide similar training programmes and campaigns. Collaboration is essential for teaching to be effective. Moreover, the competence level of citizens is significantly influenced by the citizen's own resources and interest in cybersecurity.[317]

IT is a compulsory and separate subject starting in the first grade of basic education and continuing in secondary education. Cybersecurity is taught as part of the subject throughout comprehensive school.[318] According to experts, the amount of cybersecurity education provided in comprehensive school is not yet sufficient.[319] Higher education in the field of cybersecurity is offered at several different universities, including the University of Aegean, Athens University of Economics and Business and the University of Piraeus.[320]

The Greek Safer Internet Centre (SIC) was established in 2016 with the support of the Foundation for Research and Technology – Hellas (FORTH). It is part of the international Insafe, INHOPE and Better Internet for Kids networks supported by the European Commission. The SIC has been responsible for much of the schools' cybersecurity education materials and awareness campaigns since 2016. The main target groups are children,

young people, parents and teachers, but materials are also available for citizens in general. The SIC produces various information packages, instructional videos, lesson plans, webinars, MOOCs, articles and studies, for example. The SIC website and social media channels offer a wealth of information related to cybersecurity. The SIC has organised more than 800 visits to Greek schools, seven national Safer Internet Day events and seven national cybersecurity competitions between schools. It also has 200 ambassadors across the country. Its main partners include the Ministry of Education and Religious Affairs (Υπουργείο Παιδείας και Υρησκευμάτων), the Ministry of Digital Governance and the National Cybersecurity Authority operating under it, ENISA and the Greek Police.[321,322]

The Greek Safer Internet Centre and the Greek Cybersecurity Authority have jointly carried out cybersecurity campaigns and related educational videos. The video "Smishing" explains how to identify and protect yourself from phishing, especially if done via text messages. The "Do you know what a strong password is?" video discusses good password hygiene, while the video "Don't click – don't click" describes a situation where a senior's user account has been hacked. Viewers are instructed how to act in such a situation, how to report it and why it is useful to share the experience with family and friends. These videos are intended for all citizens.[323] The SIC is the country coordinator for ENISA's annual Cybersecurity Month in Greece. In connection with the Cybersecurity Month 2022, ENISA selected the "Treasure Hunt Games for Primary School" produced by the Greek SIC as the best educational material of the year. As a result of this recognition, the material will be translated into all the official EU languages.[324]

GRNET S.A. (National Infrastructures for Research and Technology), operating under the Ministry of Digital Governance, coordinates and implements the Digital Transformation Strategy drawn up by the Ministry. To this end, a special digital skills department, the Directorate of Digital Skills, has been set up in GRNET S.A. It is also responsible for the implementation and maintenance of the National Academy for Digital Skills platform developed by the Ministry. The platform is designed for Greek citizens, and its goal is to improve their digital skills through a variety of courses. The National Academy for Digital Skills is a free platform that brings together all private and public providers of digital education and training. The project was launched at the beginning of 2020.[325,326]

The National Academy for Digital Skills currently offers approximately 300 courses, 20 of which are related to cybersecurity. Citizens can choose the appropriate study path with the help of a self-assessment tool. GRNET S.A. also offers a Digital Citizen learning path, comprising five courses, which it has developed based on the European Commission's Digital Competence Framework for Citizens (DigComp). The path is geared to citizens who have very basic digital skills. The aim is to strengthen the digital mindset of citizens and develop their skills and attitudes so that everyone can operate in the digital environment in a productive, safe and responsible way. Courses also cover cybersecurity, including secure web browsing, good password practices, and privacy protection.[327]

The Unit of Innovative Actions and Strategy in the Cyber Crime Division is responsible for raising awareness of various forms of cybercrime and cybersecurity.[328] The target groups include citizens, businesses, public sector institutions and universities. The Unit carries out its mission in various ways. In 2021 and 2022, it organised 330 lectures and workshops for different target groups. The Unit publishes leaflets, videos and other materials on cybercrime and the dangers of the internet. Newsflashes on children's online safety are broadcast on national television and radio channels. Carmen Rouggeri, a well-known actress and author, collaborated with the Unit to create a fairy tale called Sifis the Mouse and the Internet, which deals with online risks and is aimed at children under 10 years of age. CyberKid is a constantly updated cybersecurity campaign launched by the Unit. It targets especially children, young people, parents and teachers. The campaign website has been used in schools to support IT teaching. The Panhellenic School Network has raised the profile of CyberKid, which includes, among other things, cybersecurity information and mini-games.[329,330] The CyberAlert and FeelSafe websites are aimed at citizens and businesses. The websites contain up-to-date information on cybercrime and the risks of the

internet. FeelSafe focuses on the security of electronic commerce. The sites have been created in cooperation with the police, the Ministry for Civil Protection and the ESEE trade organisation.[331]

Founded in 2017 by Manolis Sfakianakis, the Cyber Security International Institute (CSIi) is a Greek non-profit, non-governmental organisation born out of the desire to protect citizens' security. CSIi cooperates with the Greek Ministry for Civil Protection (Υπουργείο Προστασίας του Πολίτη), for example. Its mission is to provide citizens with information and training concerning new technologies and the internet, the security of IT systems and infrastructures, and the safe use of the internet and software. It encourages citizens to report any cybersecurity issues they encounter and provides them with user support. The CSIi prepares educational programmes and organises workshops, seminars and conferences across Greece and is often featured in the media. It caters especially to children, parents and grandparents. Free "Digital Academy" online courses are organised for pupils and parents, which have so far been attended by 7,000 pupils and 10,000 parents. The teaching materials are prepared by the CSIi working group, which includes experts from different fields. CSIi is currently developing a new kind of interactive tutorial called "Super Internet". The goal is to teach children and young people aged 6–16 about the dangers of the internet with the help of two superheroes – Lady Ban and Mega Block. CSIi and the mobile operator COSMOTE jointly created a campaign, #HowToVideos, featuring 20 videos. The short video clips offer easy tips on how internet users can protect themselves against online fraud and keep their personal data safe.[332,333]

In June 2021, the National Cybersecurity Authority published a Cybersecurity Handbook featuring best practices for protecting networks and information systems and supporting resilience, which is geared especially to the public sector and SMEs. The handbook also addresses the improvement of employees' cybersecurity skills and awareness.[334]

3.8.3. National characteristics

In 2018 and 2019, the Greek Safer Internet Centre (SIC) and the Foundation for Research and Technology (FORTH) conducted a large survey titled "Understanding the online behaviour and risks of children: results of a large-scale national survey on 10–18 year olds". The aim of the study was to examine children's and young people's internet use and the risks involved. The first part of the study encompassed 14,000 pupils from 400 schools, and the second part involved 13,000 pupils from 500 schools. The surveys were conducted as anonymous online surveys with the support of the Ministry of Education and Religious Affairs. The results indicated a need to improve the skills of children, young people and parents related to safe internet use. Children and young people said they mainly got advice from their own parents and siblings. The study recommends that courses dealing with internet safety and security should be incorporated more broadly and systematically into the curriculum of comprehensive school and also be extended to smaller children. According to the study, the amount of digital literacy and cybersecurity teaching currently provided as part of the comprehensive school curriculum is insufficient.[335]

Greece is home to the European Union Agency for Cybersecurity (ENISA), with offices in Athens and Heraklion.[336] Greece is considered to have one of the most comprehensive national cybersecurity strategies in the EU. The country has been ranked first in the NCSI cybersecurity index since October 2019.[337]

3.8.4. The definition of cyber citizen skills

The National Academy for Digital Skills offers the "Digital Citizen" learning path comprising five courses. It is based on the DigComp framework, which has Safety as one of its competence areas. The course topics include online navigation and information searching, digital content management, data protection and privacy, creating a digital identity, and acting as a digital citizen. Aspects discussed include passwords, online scams, phishing, social media privacy and security settings, fake profiles and data breaches.[338]

References

[314] National Cybersecurity Authority, Ministry of Digital Governance, Hellenic Republic, *National Cybersecurity Strategy 2020–2025* (2020).
[315] Ministry of Digital Governance , *Βίβλος Θηφιακού Μετασχηματισμού 2020–2025* (2021).
[316] European Commission, *Digital Economy and Society Index (DESI) 2022: Greece* (2022), 3–6.
[317] A personal communication to the researcher, 01/08/2022 and 26/11/2022.
[318] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10–58.
[319] A personal communication to the researcher, 22/06/2022, 1/08/2022 and 9/08/2022.
[320] "CYBERHEAD - Cybersecurity Higher Education Database," *ENISA*, accessed on 04/11/2022, https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/.
[321] A personal communication to the researcher, 22/06/2022.
[322] "SaferInternet4Kids.gr", accessed on November 8, 2022. https://www.saferinternet4kids.gr/.
[323] "Greece, Cybersecurity Sources", *European Cybersecurity Month*, accessed on 8 November 2022, https://cybersecuritymonth.eu/countries/greece.
"The European Cybersecurity Month 2022 Awards ,*ECSM*, accessed on November 8, 2022. https://cybersecuritymonth.eu/awards.
[325] A personal communication to the researcher, 23/06/2022.
[326] "Media Kit", *Grnet*, accessed on November 4, 2022. https://grnet.gr/en/media-kit-2/.
[327] A personal communication to the researcher, 23/06/2022.
[328] "Cyber Crime Division", *Hellenic Republic, Ministry of Citizen Protection*, accessed on 30 August 2022, http://www.astynomia.gr/index.php?option=ozo_content&perform=view&id=8194&Itemid=378&lang=EN.
[329] "Hellenic Republic, Ministry of Citizen Protection", accessed on November 22, 2022. http://www.astynomia.gr/index.php?option=ozo_content&lang=&perform=view&id=103304%20&Itemid=2646&lang=.
[330] A personal communication to the researcher, 26/11/2022.
[331] "Cyber Alert", *Cyber Crime Division*, accessed September 26, 2022. https://cyberalert.gr/.
[332] A personal communication to the researcher, 01/08/2022 and 09/08/2022.
[333] "CSIi Cyber Security International Institute", accessed on November 8, 2022. https://www.csii.gr/.
[334] Ministry of Digital Governance, National Cybersecurity Authority, *Cybersecurity Handbook* (2021), 6–52.
[335] Evangelia Daskalaki, Katerina Psaroudaki, Marieva Karkanaki & Paraskevi Fragopoulou, *Understanding the online behavior and risks of children: results of a large-scale national survey on 10–18 year olds*, Iraklion: Institute of Computer Science, Foundation for Research and Technology - Hellas (FORTH) (2020).
[336]"Contact", *ENISA*, accessed on November 21, 2022. https://www.enisa.europa.eu/about-enisa/contact.
[337] George Drivas, *CYBERSECURITY IN GREECE: Facts, Current Needs & Future Perspectives*, accessed on November 21, 2022. https://www.sev.org.gr/Uploads/Documents/53423/Cybersecurity_in_Greece_Drivas_SEV.pdf.
[338] "Ψηφιακός Πολίτης", *govgr*, accessed on November 18, 2022. https://nadia.gov.gr/.

3.9. Croatia

ITU, Global Cybersecurity Index (GCI) 2020	33/182 (Global), 20/46 (Europe)
National Cyber Security Index (NCSI) 2022	16/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	21/27

3.9.1. Strategic cyber education and training policies

Croatia's National Cyber Security Strategy dates back to 2015. One of its objectives is to raise the security awareness of all cyberspace users. Especially pupils and students at all levels of education need information about the threats of the digital world and learn to safeguard their data and use technology safely. In schools, cybersecurity studies are integrated into other subjects. Training will be increased in both curricular and extracurricular activities. Lifelong learning is taken into account by providing cybersecurity education to different groups of population. The goal is also to increase information to the general public through various campaigns.[339]

3.9.2. The current state of cyber citizen skills education and training

The provision of cybersecurity education in Croatia involves the Ministry of Education (Ministarstvo znanosti i obrazovanja), which administers education in schools, the National CERT (Nacionalni CERT) and private sector actors.[340] In 2018, a new curriculum for "Informatics" (computer science) was introduced in basic education in Croatia, that is, for primary and lower secondary school pupils aged 7–14 and upper secondary school pupils aged 15–18. The subject includes an area called "E-society", which also covers cybersecurity.[341] Studies in "Informatics" begin as an elective subject at the age of 7, continuing until the end of the 4th grade. It is a compulsory subject in lower and upper secondary school.[342,343] According to the curriculum, after primary and secondary school, pupils should master the use of computers so that they can independently, responsibly, appropriately and effectively use digital technologies and prepare to function in the digital environment in every field of life. They should also be able to develop critical thinking, creativity and innovation through ICT and communicate and collaborate effectively and responsibly in the digital environment. The goal is to ensure that pupils understand and responsibly apply safety recommendations to protect their health and comply with laws and standards when using digital technologies in their daily lives.[344,345]

The E-society studies are based on the idea that studying topics such as cybersecurity, data protection and cyberbullying develops the skills and attitudes required to operate responsibly in a digital society.[346] In the first grades of primary school, students learn to use ICT equipment carefully and responsibly and to protect their personal data. They analyse the risks that can occur when using a computer and the internet and react to them appropriately. When using internet content and services, they protect their personal data and digital reputation. Older pupils acquainted themselves with questions related to the digital footprint and cyberbullying, protecting electronic identity and user accounts and preventing hate speech. In the first grade of upper secondary school, students learn about the consequences of malware, cyber attacks and identity theft, as well as the related safety guidelines.[347]

No actual Master's degree education in cybersecurity is available in Croatia, but the Faculty of Electrical Engineering and Computing of the University of Zagreb (Sveučilište u Zagrebu Fakultet elektrotehnike i računarstva) offers postgraduate studies in the Specialist Study Information Security programme.[348] Individual computer security courses are offered to students by the same faculty.[349] The Faculty of Organization and Informatics of the University of Zagreb *(Fakultet organizacije i informatike Sveučilišta u Zagrebu)* also organises

postgraduate studies in Safety Management and Information Systems Audit.[350] The Zagreb University of Applied Sciences (Tehničko veleučilište u Zagrebu) offers a Graduate Professional Study Programme in Information Security and Digital Forensics.[351] The Department of Cybersecurity at Algebra University College (Visoko učilište Algebra, Katedra za kibernetičku sigurnost) organises cybersecurity courses that cover a wide range of topics in the field.[352]

CERT offers citizens *cybersecurity training in which adults can also participate.* For example, it organises webinars, conferences and courses on various topics and teaches both how to identify cyber threats and how to respond to them. The aim is to educate citizens through social media posts, online content, radio and television programmes and newspaper articles, for example. Infographics and quizzes are also used to warn about current threats.[353]

The portal maintained by CERT[354] provides citizens with diverse information and interactive content related to cybersecurity, such as games, quizzes and tests. The portal contains materials on ten different topics, ranging from digital footprints to phishing.[355]

The first national cybersecurity campaign "Naivci" was organised by CERT in 2019.[356] The goal of the campaign, presented on TV, was to educate citizens about the most common online fraud and cybersecurity threats, and featured an overly self-confident and naive user who didn't care much about cybersecurity. The 2021 sequel to the campaign used TV, Facebook, Twitter and YouTube, for example.[357]

Croatia has participated in the ECSM (European Cybersecurity Month) campaigns organised by ENISA (European Union Agency for Cybersecurity), for example, by publishing posts on social media related to digital footprint and scams, and by organising Hacknite competitions for schoolchildren.[358] In 2021, an expert panel discussion was held on social engineering, cyber hygiene and raising safety awareness.[359] The Croatian Cybersecurity Month portal[360] provides citizens with informative material, videos and infographics.

In addition to the campaigns, Croatia disseminates information in connection with specific events. The Croatian Safer Internet Centre (SIC) participates in the Safer Internet Day (SID) by preparing educational packages for schools and organisations, producing online material for children and young people and organising expert webinars and podcasts for parents, for example.[361,362]

Since the start of the war in Ukraine in 2022, the Central State Office for the Development of the Digital Society has stepped up its communication to citizens through cybersecurity workshops covering all key topics, including disinformation.[363] *In the private sector, Learning Web Skills*[364] organises courses such as *Information and Data Literacy* and *Safety'.* The courses are mainly aimed at companies and individuals who wish to change careers and enter the IT sector.

The digital learning content provided on Netica.hr. is among the broadest.[365] This colourful website for children and adults, produced by the Croatian Safer Internet Centre, offers useful material on cybersecurity. Users can also ask questions from experts on the site. The "Safe with Netica" picture book and workbook deal with practical situations and offer advice on cybersecurity. The content is designed especially for preschoolers and primary school children[366].[367] There is also an interactive book for young children called "Think and Click".[368] It is produced by the Roda Association as part of a project of the Ministry of Demographics, Family, Youth and Social Policy (Ministarstvo demografije, obitelji, mladih i socijalne politike). The Safer Internet Centre's YouTube channel has compiled videos describing basic cybersecurity problems. The videos provide children and young people with examples of the consequences that their actions may have.[369] The Safer Internet Centre has also produced a board game and an educational guide for children and parents on the security and privacy settings of social networks.[370]

*The Croatian Academic and Research Network (*Hrvatska akademska i istraživačka mreža) *CARNET* has produced a comprehensive portal of interactive learning resources on cybersecurity, which is accessible to all on the

internet. The portal is designed especially for pupils in primary and secondary school. The topics discussed include the protection of privacy and computers and the safe use of computers.[371,372,373]

"Dabrica Darka – Growing up on a Safer Internet", by Learning Associates, is an example of Croatian learning games[374]. It includes four online games on cybersecurity for pupils in grades 1–8 of comprehensive school. In addition, four handbooks have been produced for teachers and parents, which include information on how to raise parents' awareness of the opportunities offered by the internet and how to ensure that children use the internet safely. No to E-violence is a quiz application[375] designed by Safer Internet Centre and Microsoft to help young children learn the basics of cybersecurity in a fun way.

3.9.3. National characteristics

Croatia has a strong tradition in IT specialists and companies in the IT sector[376]. The country has a high level of technological competence, especially among young people and young adults[377]. Civic skills and digital and cyber skills are part of the comprehensive school curriculum.[378] A large proportion of the population is ageing, and inadequate ICT competencies have been detected among this group. Seniors are vulnerable to simple fraud. Younger generations have a relatively short time to apply the rapidly evolving technology to various needs in the real world. Croatia recognises the need to raise awareness, especially about data protection and the need to be cautious when sharing personal data in the cyberenvironment.[379] Cybersecurity is considered a common concern for Europe, which requires joint efforts. Teaching material related to cybersecurity should be up-to-date and include current threats and opportunities. The learner's age should be taken into account in its implementation, and both theory and practice should be included. A HyFlex implementation could be used in different teaching environments.[380]

At the time of this research, Croatia is working on a strategy called *Digital Croatia 2032,* which will also include cybersecurity and the development of civic skills, from the perspective of both individuals and businesses.[381]

3.9.4. The definition of cyber citizen skills

Croatia does not have national frameworks for cybersecurity competence. It complies with either EU or international frameworks and certifications such as the EU Digital Competences Framework for Citizens (*DigComp* 2.2) and SELFIE for TEACHERS, a free self-assessment tool for primary and secondary school teachers managed by the European Commission. It enables teachers to assess their own cybersecurity skills, for example.[382,383] The curriculum contains some definitions of skills related to cybersecurity. It states that every citizen using electronic services (e-Citizen) should understand the meaning of personal data and how they can be protected. Citizens should also know how to protect themselves from fraud, threats and cyberbullying, and how to react to inappropriate behaviour, how to respect other people's privacy and where to seek help if they come across inappropriate content or people.[384,385]

References

[339] Government of Croatia, *The National Cyber Security Strategy of Republic of Croatia* (2015), 7, 24–25.
[340] A personal communication to the researcher, 27/09/2022.
[341] A personal communication to the researcher, 14/09/2022.
[342] A personal communication to the researcher, 27/09/2022.
[343] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 119.
[344] Lidija Kralj, *New Informatics curriculum—Croatian tradition with world trends*. *2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, IEEE (2016), 1.
[345] Ministry of Science and education of Croatia. *Curriculum of the Teaching Object Informatica for Primary Schools and Gymnasiums* (2018).
[346] A personal communication to the researcher, 14/09/2022.
[347] Ministry of Science and education of Croatia, *Curriculum of the Teaching Object Informatica for Primary Schools and Gymnasiums*, (2018).
[348] "Information security", *University of Zagreb*, accessed on 9 December 2022, https://www.fer.unizg.hr/studiji/specijalisticki_studiji/is.
[349] "Computer security", *University of Zagreb Faculty of Electrical Engineering and Computing*, accessed on December 9, 2022. https://www.fer.unizg.hr/predmet/comsec.
[350] "Specijalist Informacijske Sigurnosti", *University of Zagreb Fakultet organizacije i informatike*, accessed on December 9, 2022. https://usris.foi.hr/pocetna.
[351] "Graduate Professional Study in Information Security and Digital Forensics", *Zagreb university of applied sciences*, accessed on December 9, 2022. https://www.tvz.hr/studiji/diplomski/spec-isecen/.
[352] "Department courses", *Algebra University College*, accessed on December 9, 2022.https://www.algebra.hr/visoko-uciliste/en/for-students/departments-and-teachers/department-of-cyber-security/5.
[353] A personal communication to the researcher, 03/05/2022.
[354] "Ne Budi i Ti Hrvatski Naivac", *National CERT Croatia*, accessed on November 26, 2022. https://www.naivci.hr/#Uvod.
[355] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 95.
[356] "Ne Budi i Ti Hrvatski Naivac", *National CERT Croatia,* accessed on October 24, 2022. https://www.naivci.hr/#Uvod.
[357] ENISA, *Raising Awareness of Cybersecurity as a Key Element of National Cybersecurity Strategies* (2021), 27, 39.
[358] ENISA, *European Cybersecurity Month (ECSM) 2020* (2021), 46.
[359] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 96.
[360]"Cybersecurity Material", *ENISA,* accessed on 24 October 2022, https://cybersecuritymonth.eu/resources?country[]=HR&perPage=24&reqPage=1&searchText=&sortOrder=descending.
[361] ENISA, *Raising Awareness of Cybersecurity as a Key Element of National Cybersecurity Strategies* (2021), 27.
[362] "About Our SID Activities", *European schoolnet*, accessed on October 24, 2022. https://www.saferinternetday.org/in-your-country/croatia.
[363] A personal communication to the researcher, 09/08/2022.
[364] "Areas and Modules", *Learning Web Skills*, accessed on October 24, 2022. https://learningwebskills.com/index.php/areas-and-modules/.
[365] "I'm Netica!", *Croatian Safer Internet centre*, accessed on October 25, 2022. http://www.netica.hr/.
[366] "Sigurni s Neticum", *Croatian Safer Internet centre*, accessed on October 26, 2022. http://netica.hr/materijali/Slikovnica_web.pdf.
[367] "Sigurni s Neticum Radna Bilježnica Sigurnosti Na Interneta", *Croatian Safer Internet Centre,* accessed on October 26, 2022. http://netica.hr/materijali/Netica_rb_web.pdf.
[368] "Interaktivna Slikovnica Razmisli Pa Klikni Za Lakši Razgovor o Izazovima Interneta", *Roda -association,* accessed on October 26, 2022. https://www.roda.hr/udruga/projekti/razmisli-pa-klikni/interaktivna-slikovnica-razmisli-pa-klikni-za-laksi-razgovor-o-izazovima-interneta.html.
[369] "Prijavi i Zaustavi",*Croatian Safer Internet centre*, accessed on October 26, 2022. https://www.youtube.com/channel/UCOGImLmHlBh2wwE7eWPyj6Q.
[370] "Dan Sigurnijeg Interneta", *Croatian Safer Internet centre*, accessed on October 26, 2022. https://csi.hr/dan-sigurnijeg-interneta/.
[371] "6. Ispravno i Odgovorno Koristenje Racunala", *Croatian Academic and Research Network – CARNET*, accessed on October 26, 2022. https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/c4e1aebf-48e0-4d92-b6a9-0716a4e1c740/html/430_ispravno_i_odgovorno_koristenje_racunala.html.
[372] "5. Internet", *Croatian Academic and Research Network – CARNET*, accessed on October 26, 2022. https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/c9d3bbb7-0fb8-45a8-ba91-4175fca0fc8a/html/538_internet.html.
[373] "1. Racunalo i Mreza", *Croatian Academic and Research Network CARNET*, accessed on October 26, 2022. https://edutorij.e-skole.hr/share/proxy/alfresco-noauth/edutorij/api/proxy-guest/c9d3bbb7-0fb8-45a8-ba91-4175fca0fc8a/html/538_internet.html.
[374] "Dabrica Darka – Growing up on a Safer Internet", *The association Learning Associates*, accessed on 26 Octobber 2022, https://ucitelji.hr/dabrica-darka-growing-up-on-a-safer-internet/.
[375] "Što Je e-Nasilje?", *Croatian Safer Internet centre,* accessed on October 26, 2022. http://www.netica.hr/upoznajmo-i-prepoznajmo-e-nasilje/.
[376] A personal communication to the researcher, 14/09/2022.
[377] A personal communication to the researcher, 09/08/2022.
[378] "Young Croats Have The Best Digital Skills In Europe", *Total Croatia news,* accessed on 26 October 2022, https://www.total-croatia-news.com/news/45053-young-croats-have-the-best-digital-skills-in-europe.

[379] A personal communication to the researcher, 03/05/2022.
[380] A personal communication to the researcher, 14/09/2022.
[381] A personal communication to the researcher, 09/08/2022.
[382] A personal communication to the researcher, 14/09/2022.
[383] "SELFIE for TEACHERS", *The European commission*, accessed on December 9, 2022. https://education.ec.europa.eu/selfie-for-teachers.
[384] Kralj, *New Informatics curriculum*, 3.
[385] Ministry of Science and education of Croatia, *Curriculum of the Teaching Object Informatica for Primary Schools and Gymnasiums* (2018).

3.10. Cyprus

ITU, Global Cybersecurity Index (GCI) 2020	41/182 (Global), 26/46 (Europe)
National Cyber Security Index (NCSI) 2022	37/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	20/27

3.10.1. Strategic cyber education and training policies

Cyprus published its Cybersecurity Strategy in 2020. It emphasises the responsibility of society at large for safer internet use. Investments must be made in the development of cybersecurity awareness and a security culture across society. The active commitment of various stakeholders and authorities (for example CSIRT-CY (Computer Security Incident Response Team), the police (Αστυνομία Κύπρου), and the Cyprus Pedagogical Institute (CPI) (Παιδαγωγικό Ινστιτούτο Κύπρου)) to awareness-raising activities is important. Citizens should be informed about the risks and precautions, especially those related to internet services. Another goal is to facilitate the development of cybersecurity skills in all areas of the education system. The creation of information material and the use of material from external sources, such as ENISA (The European Union Agency for Cybersecurity) and Safer Internet for Kids, are also considered important. Continuous communication is required, and different forms of communication must be used to reach the general public. The aim is to create a culture of creative and safe internet use.[386]

3.10.2. The current state of cyber citizen skills education and training

In Cyprus, cybersecurity skills and training are mainly promoted by the Digital Security Authority (DSA) (Αρχή Ψηφιακής Ασφάλειας), which also includes CSIRT-CY, the Cyprus Ministry of Education, Sport and Youth (Υπουργείου Παιδείας, Αθλητισμού και Νεολαίας) and local public and private universities.[387]

In primary and secondary education, safe internet use is the responsibility of the CPI, which also sees to the guidelines and practices concerning responsible internet use. The inclusion of internet safety issues in the school curriculum, the organisation of workshops for pupils, teachers and parents, as well as presentations at conferences and events are examples of the CPI's core tasks.[388] Digital skills education is integrated into other compulsory subjects in primary education, and some schools have a separate subject called Informatics, which is compulsory or elective, depending on the school. In lower secondary education, learning objectives have been defined for the DigComp Safety competence area, which is taught in Informatics/Computer Science classes.[389]

A curriculum concerning new technology was drawn up for the 5th and 6th grades of comprehensive school in 2019. It comprises a separate subject, including "Health Education – Home Economics / Design and Technology – New Technologies". This addition is expected to strengthen the mainstreaming of digital skills and digital/media literacy in all school subjects. In the new curriculum, topics related to cybersecurity include Cyberbullying / Video – Online Games (5th graders) and Information – Misinformation / Personal Data and Digital Identity (6th graders). [390,391] Pupils in upper secondary school have also studied ECDL (European Computer Driving Licence) modules, which include eSafety questions.[392]

In upper secondary education, informatics/computer science is compulsory for one year and the lessons address safety topics. Learning objectives have been defined for the DigComp competences of Protecting personal data and privacy and Protecting health and well-being.[393]

Master's degrees in cybersecurity are offered by The Open University of Cyprus (Ανοικτό Πανεπιστήμιο Κύπρου): MSc programme in Computer and Network Security; The University of Central Lancashire Cyprus (UCLan Cyprus): MSc Cybersecurity; and the European University of Cyprus (Ευρωπανκό Πανεπιστήμιο Κύπρου): MSc in Cybersecurity at EUC.[394]

Cybersecurity training for citizens is based on the idea of preparing different training materials for different age groups, depending on the threats relevant to each group. For example, the website of the Internet Safety Awareness Centre lists the age groups to be taken into consideration in training (children, young people, adults).[395] The EU's positive impact is clearly visible in the cybersecurity training of Cyprus. The following paragraphs describe the Cyprus Safer Internet centre – CYberSafety, and Helpline and Complaints Hotline 1480 projects of the Ministry of Education, Sport and Youth, which offer advisory and support services on the safe, responsible and ethical use of the internet and digital technologies to children, young people, parents, teachers and the wider community.[396]

The Cyprus Safer Internet Centre – CYberSafety[397] receives EU funding and operates as part of the Better Internet for Kids project. It fosters cooperation between key national stakeholders to promote a safe internet culture. The aim is to support and strengthen citizens' activities in the digital society. The Awareness Centre[398] supports the work of the Safer Internet Centre by developing varied educational and information material, resources and tools, as well as by organising campaigns to teach children, young people, parents, carers and teachers how to stay safe online. The Awareness Centre works closely with children and young people to motivate them to share their ideas, suggestions and views on the creative and safe use of digital technologies and the internet. Helpline/Hotline services also support the Safer Internet Centre's operations. The goal of Helpline[399] is to ensure that everyone has access to expert advice on questions related to the use of digital technology and the internet. The members of the Cypriot CYberSafety youth panel[400] act as ambassadors of best practices and actions, aiming to create innovative resources and disseminate information about safe internet use to young people and other groups involved in the activities.

"Young coaches for the internet"[401] is an annual programme designed to educate pupils on safe internet use and help them support their school, as well as the wider community, in cybersecurity matters. Another annual programme in Cyprus, "eSafe schools"[402], trains teachers to strengthen the cybersecurity culture in their community and school unit. Through the programme, schools can receive a Safety label based on their own level of digital safety.[403,404]

The CPI's Educational Technology Department offers a number of programmes and activities each year where primary, secondary, and technical schools, and their teachers and pupils have the opportunity to participate in designing and implementing internet security, strengthen their digital skills, and promote training in creative and safe internet use in and outside their own school.[405]

In the private sector, cybersecurity and digital literacy courses for children and young people are organised, for example, by Logischool. The *"Digital discovery 113*" course covers internet safety, netiquette and online communication.[406] *Cybersecurity-related studies for adults are offered in the private sector by, for example, the Emphasys centre, which also offers ECDL training.[407] The School of Certified Professionals (SCP)* also organises cybersecurity courses and certification, as well as an online course called *"Introduction to Cybersecurity"* open to all citizens.[408]

Universities also organise cybersecurity seminars and lectures for non-experts and participate in campaigns.[409] For example, the 2021 ECSM (European Cybersecurity Month) programme included a webinar for seniors organised by European University Cyprus. An event on cyberbullying and hate speech targeted at young people was organised by the Center for Social Innovation (CSI). During the ECSM campaign, infographics, videos and material were published on the organisation's social media channels.[410,411] The Cyprus Safer Internet Centre organises courses, workshops, presentations and events for pupils, teachers and parents during the Safer

Internet Day. Internet awareness is promoted through various channels, including radio programmes and magazines.[412,413,414]

The Central Bank of Cyprus (Κεντρική Τράπενα της Κύπρου), the Association of Cyprus Banks (Σύνδεσμος Τραπεών Κύπρου), the police and the DSA organise joint campaigns. For example, the 2021 Aspis (Information Safety and Information Security) campaign provided information to the general public about methods commonly used by scammers to steal personal data and banking information.[415]

Various educational games are being integrated into school activities to support learning objectives.[416] For example, the Greek-language 3D game *"eFollowMe"* is geared towards pupils in lower and upper secondary school. The game strives to raise awareness of the digital footprint by drawing the player's attention to, for example, the use of cookies and the methods of communication in social networks. The game is available for the Windows and Mac operating systems.[417]

3.10.3. National characteristics

In Cyprus, the positive impact of the EU is reflected not only in the Cyprus Safe Internet Centre – CYberSafety[418] project, but also in the number of Erasmus courses. The Emphasys centre[419], Dora education institute[420] and Civic computing[421] organize cybersecurity training for teachers and young people.

The establishment of the DSA has been crucial in significantly enhancing the country's cybersecurity capabilities and safeguarding society. CSIRT, part of the DSA, and university representatives meet as required and participate in the preparation of events with a view to raising citizens' cybersecurity awareness.[422]

TheCyprus Cyber Security Challenge[423] is a major event in Cyprus. The Cyprus national team for the annual European Cybersecurity Challenge is selected there for further training. The CYberSafety summer camps offer experiential activities related to good cybersecurity practices to young people. In turn, the CPI organises an annual competition in which students produce short videos in line with the Safer Internet Day campaign slogan.[424]

As recommended by an expert in Cyprus, cybersecurity training material should be engaging, cover all learning styles and focus on key threats to citizens.[425]

3.10.4. The definition of cyber citizen skills

In Cyprus, lower and upper secondary schools use the DigComp framework for providing cybersecurity education.[426] The Cybersecurity Strategy specifies the safe use of the internet, the protection of personal data, appropriate behaviour in cyberspace and the protection of children on the internet as important cybersecurity skills. Awareness of cybersecurity threats and risks and their impact on society is vital. Awareness of these matters helps citizens and companies learn to behave in the online world and protect themselves from typical risks.[427] When asked about the definition of cyber citizen skills, experts in Cypriot responded as follows: (1) it is important for citizens to understand the basics of cyber threats relevant to them and to know how to apply the best practices to protect their data and systems[428]; (2) cyber citizen skills and digital skills are defined as the skills that citizens need to use the internet appropriately and detect dangers on the internet.[429]

References

[386] Republic of Cyprus, State department of research innovation and digital politics, *Cyber Security Strategy of the Republic of Cyprus 2020*, 17, 38–40, 47.
[387]Jason R.C. Nurse , Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 45.
[388] Maria Bada ja Ioannis Agrafiotis, *Cybersecurity Capacity Review of the Republic of Cyprus*, Global Cyber Security Capacity Centre (2017), 54.
[389]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 119.
[390] A personal communication to the researcher, 17/10/2022.
[391] Department of Educational Technology Cyprus Pedagogical Institute, *Αξιοποίηση των Ψηφιακών Τεχνολογιών για τη Μάθηση - Ψηφιακή Ικανότητα* (2019), 119.
[392] Emphasys Centre and ANT Limited, *Media and digital literacy report template* (2018), 4.
[393] European Commission, *Digital Education at School in Europe,* 119.
[394] "Cyberhead-Cybersecurity higher education database", *ENISA*, *accessed on December 7, 2022. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?search=cyprus.*
[395] A personal communication to the researcher, 22/09/2022.
[396] A personal communication to the researcher, 17/10/2022.
[397] "Cyprus Safer Internet Centre", accessed on 7 November 2022, https://www.betterinternetforkids.eu/sic/cyprus.
[398] "Internet Safety Awareness Centre," *Cyprus Pedagogical institute*, accessed on November 7, 2022. http://internetsafety.pi.ac.cy.
[399] "The CyberSafety project. Helpline 1480" *Cyprus pedagogical institute*, accessed on November 10, 2022. https://www.cybersafety.cy/helpline.
[400] "The CyberSafety project. Cyber Safety Youth Panel", *Cyprus Pedagogical Institute*, accessed on November 27, 2022. http://www.cybersafety.cy/youth-panel.
[401] "Young Coaches for the Internet", *Department of Educational Technology of the Cyprus Pedagogical Institute*, accessed on November 10, 2022. https://youngcoaches.pi.ac.cy/.
[402] "Safe School for the Internet Programme", *Department of Educational Technology Cyprus Pedagogical Institute*, accessed on November 11, 2022. https://esafeschools.pi.ac.cy/.
[403] "eSafetyLabel", *European schoolnet,* accessed on November 8, 2022. https://www.esafetylabel.eu/.
[404] A personal communication to the researcher, 17/10/2022.
[405] A personal communication to the researcher, 17/10/2022.
[406] "DIGITAL DISCOVERY 113 COURSE", *Logischool*, accessed on September 29, 2022. https://www.logiscool.com/en-cy/programs/digital-discovery-113.
[407] "ECDL - European Computer Driving Licence", *Emphasys centre*, accessed on November 10, 2022. https://emphasyscentre.com/education/ecdl-european-computer-driving-licence/.
[408] "Security", *School of certified professionels*, accessed on November 10, 2022. https://scp.ac.cy/.
[409] A personal communication to the researcher, 02/06/2022.
[410] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 97, 99.
[411] "European Cybersecurity Month Cyprus", *ENISA*, accessed on 21 October 2022, https://cybersecuritymonth.eu/countries/cyprus.
[412] "Safer Internet Day 2022", *Cyprus pedagogical Institute*, accessed on 10 November 2022, https://internetsafety.pi.ac.cy/safer-internet-day/SID2022/.
[413] "Cyprus Safer Internet Centre CYberSafety About Our SID Activities", *European Schoolnet*, accessed on October 21, 2022. https://www.saferinternetday.org/in-your-country/cyprus.
[414] A personal communication to the researcher, 17/10/2022.
[415] "Campaign Launched to Boost Cyber Security", *The CyprusMail,*accessed on October 21, 2022. https://cyprus-mail.com/2021/07/30/campaign-launched-to-boost-cyber-security/.
[416] A personal communication to the researcher, 22/09/2022.
[417] "eFollowMe About the Game", *University of Cyprus*, accessed on October 21, 2022. http://efollowme.cs.ucy.ac.cy/.
[418] "CYberSafety", *Cyprus Pedagogical Institute*, https://cybersafety.cy/.
[419] "Online Safety and Internet Addiction – Think before You Click!", *Emphasys Centre*, accessed on October 11, 2022. https://erasmuscoursescyprus.com/courses/online-safety-and-internet-addiction/
[420] "*Cybersecurity Education for Online Safety", Dorea educational institute*, accessed on August 10, 2022. https://dorea.org/erasmuscourses/cybersecurity-education-online-safety/.
[421] "eSkills 4All", *Civic computing*, accessed on September 29, 2022. https://eskills4all.eu/index.php/about.
[422] A personal communication to the researcher, 02/06/2022.
[423] "Cyprus Cyber Security Challenge", *The Cyprus Computer Society (CCS)*, accessed on October 21, 2022. https://ccsc.org.cy/#home.
[424] A personal communication to the researcher, 17/10/2022.
[425] A personal communication to the researcher, 22/09/2022.
[426]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 125.
[427] Republic of Cyprus, State department of research innovation and digital politics, *Cyber Security Strategy of the Republic of Cyprus* 2020, 38–39, 45–46.
[428] A personal communication to the researcher, 22/09/2022.
[429] A personal communication to the researcher, 17/10/2022.

3.11. Latvia

ITU, Global Cybersecurity Index (GCI) 2020	15/182 (Global), 37/46 (Europe)
National Cyber Security Index (NCSI) 2022	25/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	17/27

3.11.1. Strategic cyber education and training policies

Latvia's cybersecurity strategy dates back to 2019. It emphasises the importance of all citizens being aware of the risks to which they are exposed in the online environment and of the measures that can prevent exposure. In order to ensure cybersecurity, it is crucial that every person is aware of security issues in their daily lives and that they are vigilant in this respect. The aim is to raise public awareness of cybersecurity by developing age-specific guidelines and teaching materials, as well as by organising campaigns on social media security. More challenging and in-depth training on cybersecurity topics is offered to specific target groups. In addition, students and teachers must be made better aware of information security, privacy protection and reliable online services. More support should be provided for raising cybersecurity awareness among Latvian children and young people, for example, through non-formal education, games and competitions.[430]

3.11.2. The current state of cyber citizen skills education and training

In Latvia, basic education in information technology begins in primary school and continues in secondary school.[431] "Informatics" is one of the compulsory subjects in lower secondary school. In upper secondary education, IT education is integrated into other compulsory subjects. The curricula of comprehensive and secondary education include learning objectives for the "Protecting personal data and privacy" competency in DigComp's Safety competence area.[432]

The National Centre for Education (Valsts izglītības satura centrs) began developing a new curriculum for basic education in October 2016 as part of the European Social Fund project "Competence Approach to Curriculum" (School2030). The rapid development of digital content and its consumption was one of the starting points for development work. New communication platforms, the deterioration of information security in the information environment and the risks of unreliable information have increased the need to focus on knowledge, skills and attitudes that have hitherto been less emphasised, such as digital literacy and media literacy.[433] Critical thinking, cybersecurity and media literacy are therefore an integral part of the curriculum at all levels of education: it is important for students to understand the importance of information security and privacy protection and to master the use of reliable electronic services. These aspects are included in the content of different subjects and in the transversal skills of basic education. Examples of topics include how to create a digital identity and use social media[434]responsibly[435].[436]

For example, in Social and Civic Learning, at the end of the 3rd grade, pupils can identify facts from the information available in different media. At the end of the 6th grade, pupils can critically evaluate and use the information provided by various media and historical sources. They examine how organisations and people shape their digital identities and determine what a digital identity consists of. They use social media responsibly. At the end of the 9th grade, pupils can analyse and explain how the media reflect and influence people's political, social and aesthetic views and beliefs. They consult different sources and their own and others' experiences to find criteria for a well-planned digital identity, and responsibly create a digital identity.[437]

Master's degrees in cybersecurity are offered by three universities: the BA School of Business and Finance (Banku augstskola) offers a Professional Master's Degree programme in Cybersecurity Management[438], Riga Technical University (Rīgas Tehniskā universitāte) offers a study programme in Cybersecurity Engineering[439] and Vidzeme University of Applied Sciences (Vidzemes Augstskola) a Master's degree programme in Cybersecurity Engineering[440].

CERT.LV is Latvia's central cybersecurity institution, operating under the Ministry of Defence (Latvijas Republikas Aizsardzības ministrija). It provides information and training to the general public.[441] For example, before major events such as elections, it carries out information campaigns. It also publishes cyber weather reports on Latvian cyber events on social media.[442]

The*Zemgale Region Human Resource and Competence Development Centre ZRKAC (*Zemgales reģiona kompetenču attīstības centrs*)* is a municipal training institute aiming to provide lifelong learning to citizens. The institute organises courses on "Cybersecurity, computer systems and software" in its own region.[443] The Latvian Employment Agency (Nodarbinātības valsts aģentūras) provides IT training to jobseekers.[444] In the private sector, Baltic Computer Academy[445] also offers courses on cybersecurity suitable for ordinary computer users. NIC (Network Information Centre) has developed a free online course *"The Cybersecurity Basics".*[446] It is intended to serve as an introduction for people with no previous technical background. *Latvians can also take part in the Cyber Defence Awareness online course offered by the CCDCOE (The NATO Cooperative Cyber Defence Centre of Excellence)*[447]*, which* aims to raise awareness of cybersecurity risks and measures to mitigate these risks.

A training portal, macibas.mana.latvija.lv,[448] has been developed in the project "Do it digitally" (2018–2022). The project is managed by the Ministry of Environmental Protection and Regional Development VARAM (Vides aizsardzības un reģionālās attīstības ministrija). Through the website, citizens can sign up for the free online course "Distance learning programme for the development of digital skills in society"[449], which focuses on topics such as digital identity, internet security and critical literacy. "Distance learning program for digital agents"[450] is a course that offers participants the opportunity to become "digital agents" who advise others on the use of e-services. It also includes topics on safety and critical thinking and literacy.

In recent years, various cybersecurity-related campaigns for citizens have been organised in Latvia. For example, the Latvian Finance Association (Finanšu nozares asociācija) and Mastercard have organised "Viedpircējs" (Smart shopper) online shopping campaigns[451]. The Latvian Finance Association was also among the organisers of the "Neuzķeries! Esi gudrāks par krāpniekiem!" (Don't get caught! Be smarter than fraudster) campaign.[452] The "Esi reāls" (Be real) campaign focused on promoting critical thinking on social media. It was organised by the Consumer Rights Protection Centre (Patērētāju tiesību aizsardzības centrs).[453] The"Digitālās drošības ceļvedis' (Digital security roadmap) campaign[454] was carried out by TET, a telecommunications and internet service provider. The campaign resulted in a Digital Security Guide openly available online that provides advice on protecting digital identities, devices and personal information. The portal contains information for both the general audience and information addressing young people, as well as a survey for testing one's cybersecurity skills.[455]

"Superheroes do not get lost" and "Superheroes on the Internet" are campaigns addressing children, parents and teachers, organised by the Latvian State Police (Valsts policija) and partners. It is important to pay attention to children's safety on the internet.[456] The portal, managed by the police, contains educational materials for children of different ages. In connection with the campaign, a board game called "Vaifija spēle"was designed for primary school pupils. Schools can order a limited number of games free of charge.[457]

The Latvian government has organised digital security initiatives to share awareness and good practices, including the Safer Internet Day and ECSM (European Cybersecurity Month)[458] For example, during the Safer Internet Day, schools have been provided with campaign-related materials that teachers have passed on to pupils.[459] The annual Digital Week[460] is a national information and awareness campaign that promotes digital

skills. It is coordinated by the Latvian Information and Communications Technology Association LIKTA Latvijas Informācijas un komunikācijas tehnoloģijas asociācija) in cooperation with VARAM. The campaigns have also addressed issues related to digital identity, safety and security, and critical thinking.[461]

The Esidross.lv portal[462] maintained by CERT.LV contains useful advice on cybersecurity and instructions on the safe use of digital devices. The topics discussed include personal data management and privacy, and the security of devices, software and social networks. In addition, the portal provides advice on how to talk to children about internet safety. Information about the most common types of threats, as well as recommendations for avoiding them and solving problems serve as concrete assistance for cybersecurity management. The Mana.Latvija.lv portal contains instructions on e-transactions for citizens. The site is operated by VARAM. The website has a section on "Internet safety" (Drošība internetā), with tips on the safe use of the internet and mobile devices and on personal data protection, as well as advice on where to seek help in case of fraud, for example.[463]

In Latvia, particular attention is paid to the improvement of critical literacy. One example of this is an interactive game related to logic errors. It has been translated by the Latvian Debate Association "Quotu domā?" and is available to all.[464] The game helps identify fake media messages that contain logic errors.

3.11.3. National characteristics

In Latvia, cyber citizen skills are taught to some extent at school. Different age groups are also considered in the curriculum for basic education, which includes a separate module on digital competence. Nevertheless, cybersecurity skills need to be updated.[465] The challenge in this is finding the best way to reach out to citizens and organise a good awareness campaign.[466] A shortage of staff and funding is slowing down efforts to raise awareness.[467] In the future, the aim is to link cybersecurity education at schools to civil defence training. According to the *State Defence Concept*[468], cybersecurity should be part of the curriculum and one of the topics of civil defence lessons. In Latvia, civil defence lessons will become compulsory in secondary schools in 2024.

In January 2023, a new national cybersecurity centre will be established in Latvia under the Ministry of Defence (Aizsardzības ministrija). Its tasks will include advising and informing public administration and the general public on cybersecurity issues.[469]

3.11.4. The definition of cyber citizen skills

The Cyber Security Strategy defines some cybersecurity skills. According to the strategy, it is important to ensure that everyone who may be exposed to phishing email scams or social engineering has an understanding of cybersecurity. All stakeholders are equally important to the security of networks and information systems. This means that everyone should be equally aware of the risks they are exposed to online and of the actions they can take to prevent such exposure. Protecting privacy and identifying reliable online services are also considered important skills.[470] One of the important skills mentioned in Going Digital in Latvia[471] is identifying and tackling cyberbullying. In schools, cybersecurity skills are defined in line with the Safety competence area of the DigComp framework throughout primary and secondary education.[472]

References

[430] Ministry of Defence of Latvia, *Cyber Security Strategy of Latvia 2019–2022,* 2019, 19–20.
[431] A personal communication to the researcher, 21/06/2022.
[432] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45, 120.
[433] A personal communication to the researcher, 21/06/2022.
[434] A personal communication to the researcher, 21/06/2022.
[435] "Skola 2030", *National Centre for Education*, accessed on November 15, 2022. https://www.skola2030.lv/lv.
[436] OECD, *Going Digital in Latvia*, OECD Reviews of Digital Transformation, (Paris: OECD Publishing, 2021), 101.
[437] A personal communication to the researcher, 21/06/2022.
[438] "Professional Master's Degree in Cybersecurity Management", Banku augstskola, accessed on December 1, 2022. https://www.ba.lv/studies/program/cybersecurity-management/.
[439] "Cybersecurity Engineering," *Riga technical university*, accessed on December 1, 2022. https://international.rtu.lv/masters-studies/cybersecurity-engineering/.
[440] "Professional Master's in cybersecurity engineering", *Vidzeme University of Applied Sciences,* accessed on December 1, 2022. https://va.lv/en/study-here/masters-degree/cybersecurity-engineering/about-programme.
[441] "CERT.LV lectures in schools and state and municipal institutions in 2022", *CERT.LV*, accessed on November 16, 2022. https://cert.lv/lv/2022/01/cert-lv-lekcijas-skolas-un-valsts-un-pasvaldibu-iestades-2022.
[442] ENISA, *Raising Awareness of Cybersecurity: A Key Element of National Cybersecurity Strategies* (2021), 18–20.
[443] "Courses", *Zemgale Region Human Resource and Competences Development Centre*, accessed on November 15, 2022. https://www.zrkac.lv/en/index.php?view=en&id=64.
[444] A personal communication to the researcher, 21/06/2022.
[445] "Course catalogue", *BDA*, accessed on November 16, 2022. https://www.bda.lv/bda4/en/Catalog.
[446] "Free online course 'Cybersecurity Basics'", *NIC*, accessed on November 15, 2022. https://www.nic.lv/en/free-online-course-cybersecurity-basics.
[447] "Cyber Defence Awareness," CCDCOE, accessed on November 16, 2022. https://ccdcoe.org/training/cyber-defence-awareness-e-course/.
[448] "Welcome to the e-learning environment!", *Ministry of Environmental Protection and Regional Development*, accessed on November 17, 2022. macibas.mana.latvija.lv.
[449] "Distance learning programme for the development of digital skills in society", *Ministry of Environmental Protection and Regional Development*, accessed on November 17, 2022. https://macibas.mana.latvija.lv/courses/course-v1:VARAM+SAB101+2022_02/about.
[450] "Distance learning program for digital agents", *Ministry of Environmental Protection and Regional Development*, accessed on 16 November 2022, https://macibas.mana.latvija.lv/courses/course-v1:VARAM+DAT101+2022_02/about.
[451] "Education", *Latvian Finance Latvia Association*, accessed on November 18, 2022. https://www.financelatvia.eu/viedpircejs/.
[452] "Neuzķeries! Esi gudrāks par krāpniekiem!", *Finanšu nozares asociācija*, accessed on November 16, 2022. https://neuzkeries.lv/.
[453] "Esireals",*Patērētāju tiesību aizsardzības centrs*, accessed on November 16, 2022. https://www.esireals.lv/.
[454] "Sociālajā iniciatīvā 'Digitālās drošības ceļvedis' aicina aizsargāties pret digitālajiem uzbrucējiem", *LIKTA*, accessed on 16 November 2022, https://likta.lv/socialaja-iniciativa-digitalas-drosibas-celvedis-aicina-aizsargaties-pret-digitalajiem-uzbrucejiem/.
[455] "Digitālās drošības ceļvedis", *Tet*, accessed on November 16, 2022. https://www.tet.lv/vairak/digitala-drosiba.
[456] "State Police Superheroes", *Valsts policija*, accessed on November 16, 2022. https://www.vp.gov.lv/lv/valsts-policija-supervaroni.
[457]"Play the WAIFY GAME and get five SUPER POWERS!", *Latvian Safer Internet Centre*, accessed on November 16, 2022. https://drossinternets.lv/lv/posts/view/spele-vaifija-speli-un-iegusti-piecas-superspejas.
[458]OECD, *Going Digital in Latvia*, OECD Reviews of Digital Transformation, (Paris: OECD Publishing, 2021), 135.
[459] "About our SID activities", *European Schoolnet*, accessed on November 17, 2022. https://www.saferinternetday.org/in-your-country/latvia.
[460] "Digital Week in Latvia", *Digital skills & jobs platform*, accessed on November 17, 2022. https://digital-skills-jobs.europa.eu/en/actions/european-initiatives/digital-week-latvia.
[461] "We invite you to participate in Digital Week 2022!", *LIKTA*, accessed on November 17, 2022. https://digitalanedela.lv/.
[462] "Esidrošs", *CERT.LV*, accessed on 17 November 2022, Esidross.lv.
[463] "Drošība internet", *Ministry of Environmental Protection and Regional Development*, accessed on November 17, 2022. https://mana.latvija.lv/drosiba/.
[464] "Thou shalt not commit logic fallacies", *The school of thought*, accessed on November 17, 2022. https://yourlogicalfallacyis.com/lv.
[465] A personal communication to the researcher, 27/07/2022.
[466] ENISA, *Raising Awareness of Cybersecurity*, 45.
[467] Jason R.C. Nurse , Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 55.
[468] Ministry of Defence of the Republic of Latvia, *State Defence Concept* (2020), 1, 17.
[469] "New National Cyber Security Center set to launch next year", *LSM.lv*, accessed on August 28, 2022. https://eng.lsm.lv/article/society/defense/new-national-cyber-security-center-set-to-launch-next-year.a460484/.
[470] Ministry of Defence of Latvia, *Cyber Security Strategy of Latvia 2019–2022, 17, 19.*
[471] OECD, *Going Digital in Latvia*, OECD Reviews of Digital Transformation, (Paris: OECD Publishing, 2021), 101.
[472] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45, 120.

3.12. Lithuania

ITU, Global Cybersecurity Index (GCI) 2020	6/182 (Global), 4/46 (Europe)
National Cyber Security Index (NCSI) 2022	2/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	14/27

3.12.1. Strategic cyber education and training policies

The Lithuanian Cyber Security Strategy (2018) states that in order to strengthen the cybersecurity culture, children and young people should be provided with fundamental knowledge of cybersecurity at different levels of education, starting from kindergarten. Efforts should also be made to improve teachers' cybersecurity qualifications. This would enable them not only to better educate young people, but also to contribute to the development of society and increase general cybersecurity awareness. Research indicates that a large proportion of Lithuanians do not understand the risks of cybercrime, and therefore awareness needs to be raised among ordinary citizens. To strengthen the cybersecurity culture, it is important to effectively and regularly disseminate information about the latest threats and other factors that may threaten personal data security or expose people to cybercrime in cyberspace.[473]

3.12.2. The current state of cyber citizen skills education and training

In Lithuania, the development of cybersecurity skills is mainly promoted by schools, higher education institutions, the private sector, government institutions and the government.[474] The National Agency for Education (Nacionalinės švietimo agentūros, NŠA) is responsible for cybersecurity training in schools. It develops educational programmes for primary, lower secondary and upper secondary schools. The curriculum for basic education strongly emphasises secure internet use and communication, and in comprehensive school, pupils learn about topics related to internet security.[475] Digital competence is included in the curriculum, and digital literacy is a common competence area for everyone. The different sections of the DigComp framework's Safety competence area are included in the curriculum for comprehensive school, and the "Protection of personal data and privacy" section is also included in the curriculum for secondary education.[476]

The curriculum for grades 1 to 4 (primary education) emphasises that teachers must tell pupils about the dangers of the Internet, explain the dangers of disclosing personal data and advise them on how to avoid dangerous situations when using the internet.[477] The topic of security and fairness is discussed in *Informatics*, an elective subject taught in primary school.[478]The curriculum for the 5th and 6th grades addresses topics related to internet security in connection with the Internet and its services *module.*[479]

The cybersecurity curriculum for lower and upper secondary schools includes the Information Technology subject, which aims to teach students how to use internet resources and services legally and safely.[480] For example, in Technologies: Safe and lawful use of information and the Internet (8.2.4.), pupils learn about computer and personal data protection, copyright, communication in social networks and matters related to electronic signatures and electronic services.[481] Upper secondary education in the elective ICT (Information Communication Technology) and Engineering subjects includes the development and configuration of secure information systems, and the safe use of digital devices.[482]

Four Lithuanian universities offer Master's degree studies in cybersecurity: Vilnius Gediminas Technical University (Vilniaus Gedimino Technikos Universitetas) in "Information and Information Technology Security"[483]; Vilnius University (Vilniaus universitetas) in "Computer Modelling"[484]; Kaunas University of Technology (Kauno

technologijos universitetas) in "Information and Information Technology Security"[485]; and Mykolo Romeris University (Mykolo Romerio universitetas, MRU) in "Cybersecurity Management"[486].

The private and third sectors offer various courses and materials on cybersecurity for the adult population.[487] Some of the courses are for businesses, but CSA (Cyber Security Academy), for example, organises security awareness training courses that are also suitable for ordinary citizens.[488] Companies also carry out individual training initiatives in schools and kindergartens.[489] One option for a skills update is the *LCC Cybersecurity Bootcamp*, a cybersecurity training programme organised by LCC International University. It is especially aimed at individuals with limited IT skills who would like to prepare for a job in the cybersecurity sector.[490]

Lithuanian banks, police and libraries are active in the field of cybersecurity training. The police have organised meetings with citizens to teach them how to identify cybercrime and protect themselves against it.[491] Lithuanian banks and the Lithuanian Banking Association (Lietuvos bankų asociacija) have carried out information campaigns on phishing.[492] Libraries, in turn, have participated in the Safer Internet Day, for example, by organising interactive lectures on Zoom and providing quizzes for children and adults on the Quizziz platform.[493] Members of the *Women4cyber community* give lectures to university students and also provide training in kindergartens.[494]

The Lithuanian Safer Internet Centre promotes safer use of the internet and mobile technology. Resources are developed for different target groups: children and young people, parents and carers, teachers, social workers and instructors. The most important national campaigns are the *Safer Internet Day (SID)* and Week, and the All Digital Week. The Safer Internet Centre participates in local and national events, organises training for teachers and meetings for students. Online security is also promoted through traditional and social media.[495] One of the main media is the national Safer Internet Centre portal[496], used to disseminate resources to citizens and promote events related to safe internet use.

Some cybersecurity campaigns, such as the Local Hack Day, are organised regularly. In addition, campaigns are arranged when cybersecurity events are otherwise showcased in the media.[497] In 2019 and 2020, the Lithuanian government implemented the "Sustiprink imunitetą" (Strengthen Immunity) campaign[498], which aimed to teach people to identify and counter threats on the internet. The portal's "*Naršyk saugiai"* (Browse safely) section aims to inform people of all ages about the hidden threats on the internet. *"Atpažink melagienas"* (Recognise Liars) teaches users to recognise fake news. The portal also contains tests related to fake news and computer and phone protection.

The *"Langas į ateitį"* association coordinates the annual All digital weeks events in Lithuania. The aim is to help people of all ages with matters related to digital skills. In 2022, one of the topics was cybersecurity, including safer online behaviour, password management, secure online payment and the actions to take in a suspicious situation. The experts included financial crime prevention experts, among others.[499,500]

The project Connected Lithuania: Effective, Secure and Responsible Digital Society in Lithuania, implemented in 2018–2021, was aimed at citizens with inadequate digital skills and at young people. The project was implemented by a number of governmental bodies and actors, including the Lithuanian Ministry of the Interior *(Lietuvos Respublikos vidaus reikalų ministerija)* and the Lithuanian Communications Regulatory Authority RRT (*Lietuvos Respublikos ryšių reguliavimo tarnyba).* During the project, events for young people, courses containing cybersecurity topics, and digital literacy lessons in libraries were organised.[501] The project portal's self-study material includes topics ranging from privacy protection to critical thinking and threat identification, as well as the Kid online quiz for children and parents[502] to help identify suspicious online games and social engineering.

The Esaugumas (Security) portal is maintained by the RRT. The portal offers themes for teaching cybersecurity, ranging from more technical topics (antivirus, spyware and malware) to more privacy-focused topics and e-commerce. Users can also ask questions from cybersecurity experts.[503] "Editorial office 2030", a learning game for smart devices, aimed at developing critical thinking can be found in the Connected Lithuania project portal.[504] The portal also has a "Safer Internet" application for smartphones and tablets for testing one's

knowledge of safe online behaviour. The Kaunas Faculty of Vilnius University (Vilniaus universitetas Kauno fakultetas) has developed a game called "CTF @KnF". For older schoolchildren, there is a game called "TableTop".[505]

3.12.3. National characteristics

Cybersecurity attacks are becoming increasingly sophisticated, and Lithuania is considering whether general cybersecurity competence is increasing fast enough to bridge the gap between society's cyber defence skills and the cyber-attack skills of malicious individuals.[506] Especially the younger generation and IT specialists have better cybersecurity skills, but there are many users who do not have basic knowledge of cybersecurity, as well as very naive users who are easy targets for scams. Lithuanians also feel a need for information in the fight against fake news.[507]

Schools in the public sector face challenges in providing cybersecurity education for pupils. There are gaps in teachers' skills, and schools seem to lack a uniform system for strengthening pupils' cybersecurity skills.[508] For example, according to recommendations, the basics of cybersecurity should be taught in upper secondary school, but since teachers have considerable leeway to choose what they teach in practice, some children may not learn the basics in this field. However, on a positive note, the situation in terms of cybersecurity skills is improving every year. [509] This year, the Ministry of Defence aims to identify cybersecurity needs and shortcomings and prepare a national cybersecurity development programme that includes a proposal to improve cybersecurity education. The Ministry of Education, Science and Sport *(Švietimo, mokslo ir sporto ministerija),* NŠA and universities are working together to investigate cybersecurity issues with the aim of proposing functioning and straightforward future solutions.[510] Lithuania is actively promoting research into the application of gamification in cybersecurity education. In *TableTop* implementations, gamification is used to simulate various cybersecurity scenarios, such as critical cases related to cybersecurity for players to solve.[511]

3.12.4. The definition of cyber citizen skills

In Lithuania, DigComp has been used as a basis for the development of ICT education in comprehensive school. In the "Connected Lithuania" project, all training programmes were developed according to levels 1–2 of the DigComp framework. DigComp was also recommended for digital skillsin the Digital Agenda 2014–2020.[512]

In Lithuania, national requirements for the general public's cybersecurity skills have not yet been officially formulated, but the need for a definition of these skills in legislative documents is recognised.[513,514] A review of the curricula for cybersecurity courses indicates that they focus on technologies used to implement cybersecurity, as well as password management and ways to identify phishing and other online scams. As the majority of successful cyber attacks are made by exploiting human weaknesses, a great deal of attention needs to be paid to these aspects. It is therefore crucial to identify phishing and other forms of scams. It is also essential to understand security management processes, such as software updates and regular password changes.[515]

References

[473] Ministry of National Defence Republic of Lithuania, *National Cyber Security Strategy* (2018), 12–13.
[474]Jason R.C. Nurse, Konstantinos Adamos, Athanasios Grammatopoulos ja Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 56.
[475] A personal communication to the researcher, 14/06/2022.
[476] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 45.
[477] Nacionalinė švietimo agentūra, *Pradinio ugdymo bendroji programa (1 priedas)* (2008), accessed on November 3, 2022, https://duomenys.ugdome.lt/saugykla/bp/2016/pradinis/1_pradinio%20ugdymo%20bendroji%20programa.pdf.
[478] European Commission, *Digital Education*, 120.
[479] Nacionalinė švietimo agentūra, *Informacinės technologijos* (2008), accessed on November 3, 2022. https://duomenys.ugdome.lt/saugykla/bp/2016/pagrindinis/8_Informacines_technologijos.pdf, 17-19.
[480] A personal communication to the researcher, 14/06/2022.
[481] Nacionalinė švietimo agentūra, *Informacinių technologijų ugdymo bendroji programa* (2011), accessed on November 3, 2022. https://duomenys.ugdome.lt/saugykla/bp/2016/vidurinis/IT_7_priedas.pdf, 14-15.
[482] European Commission, *Digital Education*, 120.
[483] "Information and Information Technologies Security", *Vilnius Gediminas Technical University*, accessed on December 1, 2022. https://vilniustech.lt/for-international-students/degree-programmes-in-english-language-20222023/graduate-studies/information-and-information-technologies-security/102373?lang=2.
[484] "Computer Modelling", *Vilnius University*, accessed on December 1, 2022. https://www.vu.lt/en/studies/master-studies/computer-modelling#programme-structure.
[485] "Information and Information Technology Security," *Kaunas University of Technology*, accessed on December 1, 2022. https://admissions.ktu.edu/programme/m-information-and-information-technology-security/.
[486] "Cybersecurity Management", *Mykolas Romeris University*, accessed on December 1, 2022. https://www.mruni.eu/en/study_program/cybersecurity-management/.
[487] A personal communication to the researcher, 06/11/2022.
[488] "Security awareness training", *Cyber security academy*, accessed on October 31, 2022. https://www.cybersecurityacademy.lt/en-security-awareness.
[489] A personal communication to the researcher, 14/06/2022.
[490] "Cybersecurity bootcamp", *LCC International university*, accessed on October 31, 2022. https://lcc.lt/cybersecurity-bootcamp.
[491] A personal communication to the researcher, 14/06/2022.
[492] Maria Bada ja Carolin Weisser, *Cybersecurity Capacity Review Republic of Lithuania*, Global Cyber Security Capacity Centre 2017, 36.
[493] "Safer Internet day in Lithuanian libraries", *International Federation of Library Associations and Institutions,* accessed on 31 October 2022, https://www.ifla.org/news/safer-internet-day-in-lithuanian-libraries/.
[494] A personal communication to the researcher, 14/06/2022.
[495] "Lithuan Safer Internet Centre", *European schoolnet*, accessed on October 31, 2022. https://www.betterinternetforkids.eu/sic/lithuania.
[496] "Kurkime *saugesnį* internetą kartu", *Draugiškas Internetas*, accessed on October 31, 2022. www.draugiskasinternetas.lt.
[497] A personal communication to the researcher, 06/11/2022.
[498] "Atpažink ir atremk grėsmes internete", *Government of the Republic of Lithuania,* accessed on October 31, 2022. https://sustiprinkimuniteta.lt/.
[499] "Digital Week events 2022 in Lithuania", *Digital Skills and Jobs Platform*, accessed on 31 October 2022, https://digital-skills-jobs.europa.eu/en/latest/events/digital-week-2022-events-lithuania.
[500] "All digital weeks event in Lithuania-Invited all ages", *All digital week*, accessed on October 31, 2022. https://www.alldigitalweek.eu/all-digital-week-2022-events-in-lithuania-invited-all-ages/.
[501] "Connected Lithuania", *Digital Skills and jobs Platform*, accessed on 1,November 2022. https://digital-skills-jobs.europa.eu/en/inspiration/good-practices/connected-lithuania.
[502] "Safer Internet for Kids (quiz)", *Langas į ateitį,* https://www.prisijungusi.lt/savarankiskas-mokymasis/saugesnis-internetas-vaikams-viktorina/.
[503] "Be safe in cyberspace", *Communications Regulatory Authority of the Republic of Lithuania*, accessed on October 31, 2022. https://www.esaugumas.lt/.
[504] "A safer Internet", *Langas į ateitį*, accessed on November 1, 2022. https://www.prisijungusi.lt/savarankiskas-mokymasis/saugesnis-internetas/.
[505] A personal communication to the researcher, 06/11/2022.
[506] A personal communication to the researcher, 06/11/2022.
[507] Aelita Skaržauskienė, Monika Mačiulienė ja Ornela Ramašauskaitė, *The digital media in Lithuania: Combating disinformation and fake news, Acta Informatica Pragensia* 9.2 (2020), 1, 13-15.
[508] Rūta Valavičiūtė, *Kibernetinio saugumo kultūros vystymas Lietuvos bendrojo ugdymo mokyklose*, PhD Thesis, Mykolo Romerio universitetas (2022), 89.
[509] A personal communication to the researcher, 06/11/2022.
[510] A personal communication to the researcher, 14/06/2022.
[511] Agnė Brilingaitė, Linas Bukauskas, Virgilijus Krinickij ja Eduardas Kutka, *Environment for cybersecurity tabletop exercises, ECGBL 2017 11th European Conference on Game-Based Learning*, Academic Conferences and publishing limited, 2017.
[512] "Awareness of the DigComp framework among the CEPIS community", *Council of European Professional Informatics Societies*, accessed on 11 November 2022, https://cepis.org/digcomp-report-2021/.
[513] A personal communication to the researcher, 06/11/2022.
[514] A personal communication to the researcher, 22/11/2022.
[515] A personal communication to the researcher, 06/11/2022.

3.13. Luxembourg

ITU, Global Cybersecurity Index (GCI) 2020	13/182 (Global), 7/46 (Europe)
National Cyber Security Index (NCSI) 2022	39/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	8/27

3.13.1. Strategic cyber education and training policies

In 2021, the Luxembourg government published the National Cybersecurity Strategy IV for 2021–2025. Its three main strategic objectives are (1) to build trust in the digital world and protect human rights online, (2) to strengthen the security and resilience of Luxembourg's digital infrastructures, and (3) to develop a reliable, sustainable and secure digital economy. Measures that directly affect citizens fall especially within the first of these. Efforts to protect the rights of children and young people online will be continued by raising citizens' awareness of cybersecurity threats. This task is specifically assigned to the BEE SECURE initiative launched by the Government in 2010 and coordinated by the National Youth Service (SNJ, Service National de la Jeunesse). Under-represented groups in the cybersecurity sector, such as women, girls and people with an immigrant background, are encouraged to seek training and employment in the field. Cybersecurity matters are discussed in an inter-ministerial working group aiming to improve citizens' digital inclusion. Cybersecurity training will be developed to better meet the needs of society, and awareness of cybersecurity professions will be raised.[516]

The Ministry for Digitalisation has prepared a National Action Plan for Digital Inclusion for 2021–2024. It aims to improve digital inclusion, essential for socio-economic cohesion, counteract the digital divide of the population and support digital citizenship. The Action Plan focuses on developing digital literacy and digital citizenship to enable citizens to use digital pathways more autonomously and securely. One of the key measures is to raise cybersecurity awareness. The development of digital skills is supported from a young age, including through the digital education strategy of the Ministry of Education, Children and Youth (Ministère de l'Éducation nationale, de l'Enfance et de la Jeunesse), Einfach Digital. Digital education is offered to different skill levels and age groups in several languages. The Action Plan for Digital Inclusion pays special attention to groups that typically lack digital skills, such as seniors and people with disabilities.[517]

3.13.2. The current state of cyber citizen skills education and training

The Action Plan for Digital Inclusion includes a number of initiatives aimed at raising citizens' cybersecurity awareness. The Zesummen Digital web portal compiles information about actors promoting digital inclusion, training, materials and publications. Some of them focus on cybersecurity. The CYBERSECURITY Luxembourg website of the Ministry of the Economy provides information about public and private actors focusing on cybersecurity. The site also contains news, materials and events related to cybersecurity. The revamped Luxembourg House of Cybersecurity (LHC) (formerly SECURITYMADEIN.LU) began operating in October 2022. The objective of the organisation, operating under the Ministry of the Economy, is to promote an open and reliable cybersecurity knowledge economy. Its operations are based on cooperation between cybersecurity actors and on cybersecurity expertise accumulated over the last 20 years. The LHC provides information on various projects, such as BEE SECURE, which aims to develop citizens' cybersecurity competence. It also serves as the Luxembourg National Cybersecurity Coordination Centre (NCC), which is tasked with coordinating cybersecurity education and awareness, among other things. The CIRCL, a Computer Emergency Response Team (CERT), and the National Cybersecurity Competence Centre NC3 operate under the LHC. NC3 helps companies in particular to test and improve the cybersecurity competence of their personnel. One of the key training

methods is ROOM#42, a simulator in which participants practise cybersecurity skills in a realistic and intensive cyber attack simulation.[518,519]

Citizens' awareness of digital security practices and confidence in the digital environment will be improved through a variety of training courses, awareness campaigns and materials. This task is assigned especially to the BEE SECURE project. In its role as the Luxembourg Safer Internet Centre (SIC), BEE SECURE is also involved in the Insafe, INHOPE and Better Internet for Kids international networks. BEE SECURE aims to promote citizens' safe, responsible and positive use of new information technologies. It advises children and young people on how to use new technologies safely, supports parents, teachers and educators in providing a good role model for children and young people, and responds to seniors' growing need for support in cybersecurity matters. The main areas of activity are the development of educational content, teaching, training, counselling, awareness campaigning, monitoring and reporting of illegal content.[520]

The BEE SECURE online safety education programme for children and young people was launched in comprehensive schools in 2011. The aim of this nationwide and ongoing project is to provide schoolchildren with the skills required to use the digital operating environment safely and responsibly. Instruction is compulsory for seventh-graders, but it is also available for other age groups. In comprehensive schools, BEE SECURE education includes topics related to cybersecurity and, to some extent, media literacy. During lessons, pupils discuss topics such as the structure and functioning of the internet, cyberbullying, phishing, malware, data protection, passwords and copyright. Instruction is summed up in three main messages: 1) the internet is based on a technical infrastructure and is not a "magic thing"; 2) the internet never forgets; and 3) you are responsible for protecting yourself and your data. Since the academic year 2021–2022, secondary schools have been teaching Digital Sciences, one of the learning objectives of which is the responsible and safe use of digital technology.[521,522,523]

Teaching organised by BEE SECURE employs a variety of teaching methods and tools. As support for their instruction, teachers use PowerPoint presentations that incorporate theory in a visual format and activities that support theory, such as games, quizzes, and discussion topics. Teaching is interactive and inclusive. Storytelling is used in instruction for young children. Especially with young people, the aim is to keep discussions as informal as possible. Teachers highlight various cybersecurity risks, but allow young people to steer the discussion. Classes usually last for one-and-a-half to two hours. Teaching is available in German, French, Luxembourgish and English.[524]

In addition to formal education, BEE SECURE organises informal education and campaigning for children, young people, teachers, educators, parents, seniors and citizens in general.[525] On the Bee.lu website for children under school age, Bibi the Bee and her friends can be found in fairy tales dealing with cybersecurity themes. The site offers activities suitable for children, such as arts and crafts and colouring.[526] Silversurfer.lu is a website for seniors offering information, news and events related to cybersecurity. Silver Surfer organises discussion events for seniors focused on the safe use of new technologies. Seniors can get help with cybersecurity issues from Silver Surfer's helpline and via email.[527]

BEE SECURE and GoldenMe, a non-profit organisation, recently signed an agreement to host cyber-café events for seniors. Seniors can bring their own tablet, computer or mobile phone to the event and receive support from volunteers.[528, 529] Afternoon clubs and youth centres around the country organise informal cybersecurity instruction. DigiRallye events for 9–12-year-olds are popular. Due to the coronavirus pandemic, the event has also been organised virtually. Spots where children perform cybersecurity-related activities are set up around the venue, such as a school building. An educational package on cyberbullying has been prepared for young people with intellectual disabilities. Parents' evenings are organised where parents can ask questions about their children's digital devices and internet use. A great deal of information is also available on the BEE SECURE website.[530,531]

BEE SECURE trains its own freelance teachers for schools and youth centres, for example. In addition to the initial training, teachers participate in regular teacher meetings. According to feedback from other teachers and

parents, the concept works well. Instruction is free for schools. After each lesson, both students and teachers complete a feedback form used to continuously improve the teaching offered by BEE SECURE. Based on feedback from more than 28,000 students and more than 5,000 teachers over the period 2011–2018, this carefully designed and continuously assessed cybersecurity education offers good support to children's and young people's understanding of the topic and increases teachers' willingness to integrate cybersecurity into the curriculum. Most of the students found the teaching useful.[532,533]

The Lycée Guillaume Kroll offers a two-year cybersecurity programme after upper secondary school (Brevet de technicien supérieur en Cybersécurité).[534] The University of Luxembourg offers a Master's programme in Information System Security Management.[535] Since 2021, the Digital Learning Hub has offered IT education, including cybersecurity courses. The courses are free for the unemployed, students and government employees. The Digital Learning Hub has its own training programmes tailored to women, so that they can more easily find new opportunities in the digital field. Luxembourg Women Cyber Force, Women In Digital Empowerment and Cyberwayfinder are other projects aimed at attracting women in particular to digital tasks and cybersecurity.[536,537]

To raise cybersecurity awareness, a wide range of cybersecurity-related events are organised in Luxembourg, both online and offline, including campaigns, competitions and meetings. Cybersecurity Week Luxembourg is an annual event well-known to citizens that brings together actors from the cybersecurity ecosystem. The conference and exhibition area are open and free for everyone.[538,539]

3.13.3. National characteristics

Luxembourg is deeply committed to improving cybersecurity in the country, and efforts to raise its citizens' cybersecurity awareness began more than 20 years ago. The national cybersecurity ecosystem is based on close cooperation between public and private stakeholders. The central role of the Ministry of the Economy makes Luxembourg unique in Europe: cybersecurity is not considered merely a defence issue, but also an issue of economic importance.[540,541] Cybersecurity training is mainly provided in schools and workplaces. The special target groups are children, young people, teachers, parents, seniors and employees. A great deal of high-quality teaching material is available. The challenge is how to get all citizens to participate in training and familiarise themselves with the materials.[542]

3.13.4. The definition of cyber citizen skills

The Medienkompass is a national framework for media education, which is based on the European Commission's Digital Competence Framework for Citizens. The Medienkompass includes five areas of expertise: knowledge and information, communication and cooperation, content production, data protection and security, and the digital world. Data protection and security includes the protection of devices and the protection of data and privacy. The goal is to identify and understand the risks and threats of the digital environment (for example malware, social manipulation, identity theft) and to know the necessary security measures (for example the use of antivirus software and a firewall). In addition, everyone should know how to protect their personal data and privacy in the digital environment and be aware of their rights related to data protection.[543]

References

[516] Le Gouvernement Du Grand-Duché De Luxembourg, *National Cybersecurity Strategy IV* (2021), 8–10.
[517] Ministry for Digitalisation, *National Action Plan for Digital Inclusion, For a digitally inclusive society* (2021).
[518] Ministry for Digitalisation, *National Action Plan for Digital Inclusion, For a digitally inclusive society* (2021).
[519] A personal communication to the researcher, 25/10/2022.
[520] Le Gouvernement Du Grand-Duché De Luxembourg, *National Cybersecurity Strategy IV* (2021), 24.
[521] Aline Tiemann, André Melzer ja Georges Steffgen, *Nationwide Implementation of Media Literacy Trainings on Internet Safety* (2021), Communications, 46 (3), 394-418, https://doi.org/10.1515/commun-2021-0049.
[522] A personal communication to the researcher, 10/06/2022.
[523] Ministry for Digitalisation, *National Action Plan for Digital Inclusion, For a digitally inclusive society* (2021), 29.
[524] A personal communication to the researcher, 10/06/2022.
[525] ”BEE SECURE”, accessed on October 31, 2022. https://www.bee-secure.lu/de/.
[526] “BEE SECURE, bee.lu”, accessed on October 31, 2022. https://www.bee.lu/.
[527] “BEE SECURE, silversurfer.lu”, accessed on October 31, 2022. https://silversurfer.lu/de/.
[528] A personal communication to the researcher, 25/10/2022.
[529] “GoldenMe”, accessed on November 1, 2022. https://en.goldenme.me/.
[530] A personal communication to the researcher, 10/06/2022.
[531] “BEE SECURE”, accessed on October 31, 2022. https://www.bee-secure.lu/de/.
[532] Aline Tiemann, André Melzer ja Georges Steffgen, *Nationwide Implementation of Media Literacy Trainings on Internet Safety* (2021).
[533] A personal communication to the researcher, 10/06/2022.
[534] “BTS Cybersecurity”, *Lycée Guillaume Kroll*, accessed on October 31, 2022. https://www.lgk.lu/bts/cyb/.
[535] “Master in Information System Security Management”, *Université Du Luxembourg*, accessed on October 31, 2022. https://wwwen.uni.lu/studies/fstm/master_in_information_system_security_management.
[536] “Digital Learning Hub”, *Le Gouvernement Du Grand-Duché De Luxembourg*, accessed on October 31, 2022. https://dlh.lu/.
[537] A personal communication to the researcher, 25/10/2022.
[538] A personal communication to the researcher, 25/10/2022.
[539] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 111-114.
[540] Cybersecurity Luxembourg, *Luxembourg Cybersecurity Ecosystems, Key Insights* (2020), 4.
[541] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 111-114.
[542] A personal communication to the researcher, 25/10/2022.
[543] Script, *Medienkompass Medienkompetent lehren und lernen*, Einfach Digital (2022).

3.14. Malta

ITU, Global Cybersecurity Index (GCI) 2020	49/182 (Global), 29/46 (Europe)
National Cyber Security Index (NCSI) 2022	72/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	6/27

3.14.1. Strategic cyber education and training policies

Malta's National Cybersecurity Strategy for 2023–2026 was published in November 2022. It is a part of the overarching Digital Malta strategy and based on the cybersecurity strategy published in 2016. According to the strategy, everyone, including citizens, are responsible for protecting the cyberspace. Society as a whole must act safely and prudently online. One of the four corner stones of the strategy is cyber competence and culture which will be strengthened through various measures. Cybersecurity capacity will be improved through ongoing and extensive awareness raising programmes to promote a "safety first" culture. Cybersecurity education will be increased in both comprehensive and further education, and cooperation between educational institutions will be strengthened. Regular training on digital skills and cybersecurity competence will be provided for teachers. Cybersecurity training will be offered to employees in the public sector and important stakeholder groups because the public sector processes plenty of sensitive information. More cybersecurity training and certification opportunities will be offered to both ICT professionals and professionals in other fields as well as the management. Women will be encouraged to participate in cybersecurity projects. Sufficient support will be provided to research and innovation efforts related to cybersecurity.[544,545]

The new National eSkills Strategy 2022–2025, published in November 2022, also falls under the overarching Digital Malta strategy and builds on the National eSkills Strategy 2019–2021. The aim of the strategy is to further develop the digital skills of Maltese people. Regardless of age, sex, possible disabilities, education, financial status or ethnicity, every Maltese citizen should become a digital citizen with rights and obligations and skills to use information and communication technologies. Digital skills are not only learned through formal education, but already in early childhood and later in working life. Every Maltese citizen should have sufficient knowledge, skills and competencies to use digital tools safely and ethically. This also includes cybersecurity competence. These competencies are considered to have a significant impact on the citizens' wellbeing and resilience and foster confidence in the use of digital technologies. Pupils are entitled to education in digital literacy, starting from early childhood education to the end of primary and lower secondary education. Digital literacy will become a subject on its own. The workforce must have sufficient digital skills to do well in working life and ensure that employers remain competitive. Teachers' and students' good digital skills promote their success in digital learning environments. Citizens are encouraged to work in ICT and the digital sector.[546,547]

3.14.2. The current state of cyber citizen skills education and training

The Malta Information Technology Agency (MITA) coordinates cybersecurity issues in Malta. In 2016, it was assigned to organise and oversee campaigns and training intended for citizens which are planned in the cybersecurity strategy. Other authorities, such as the Ministry for Education, Sport, Youth, Research and Innovation, also contribute to the achievement of the goal. To fulfil the training and awareness objective, a continuous Cyber Security Malta campaign was launched. It highlights topical cybersecurity risks. In October 2022, the National Cybersecurity Coordination Centre (NCC) was launched in Malta, and the content related to Cyber Security Malta was transferred to NCC at this time. The task of the new centre is to embrace cybersecurity opportunities, raise awareness, support training programmes, encourage information sharing and collaboration,

stimulate the growth of cyber professionals, facilitate cyber investment, and provide support to the local ecosystems. MITA is responsible for NCC's operation. In addition to Malta's cybersecurity strategy, the new NCC website contains articles, news and instructions related to cybersecurity as well as information about events. NCC's social media channels raise citizens' cybersecurity awareness by regular publications. The YouTube channel publishes various videos with instructions and hints. In the video campaign of 2022, Maltese musicians share cybersecurity tips with citizens. MITA organises the annual Cyber ROOT cybersecurity conference.[548,549,550]

Informatics is taught as an independent and mandatory subject starting from lower secondary school. Informatics includes security-related learning goals that are mandatory for all.[551] Digital literacy has been defined as a key cross-curricular theme in primary and lower secondary education. Netiquette and security practices are part of digital literacy.[552] The Directorate for Learning and Assessment Programmes (DLAP) is responsible for the curriculum, teaching, assessment and monitoring of primary and lower secondary schools. DLAP participates in the BeSmartOnline! project and brings cybersecurity teaching to schools in the form of a subject called Personal, Social and Career Development (PSCD). PSCD is a mandatory subject in grades 3–11, and it includes cybersecurity. The discussed topics include digital footprint, digital citizenship, internet security, cyberbullying, digital games and critical media literacy. The classes are interactive, and the maximum number of pupils in a class is 16. The pupils sit in a circle to promote active dialogue, reflection and participation. The teachers use different teaching methods, such as games, role play and teaching in small groups. Various materials have been produced to support teaching, such as cybersecurity guides.[553]

In primary and lower secondary education, cybersecurity is taught in ethics lessons as part of the digital citizenship framework. Ethics is offered to 5–16-year-old pupils who do not participate in religion lessons. The lessons focus on the ethical values of responsible online behaviour. 5–10-year-old children are taught how to communicate responsibly on the internet, safeguarding the security and wellbeing of themselves and others, and what good password hygiene entails. The pupils are instructed how to protect themselves against cyberbullying and online predators. Teachers discuss the balance between online and offline life, reputation management, cyberbullying, sexting, hate speech and online radicalisation with 11–16-year-old pupils.[554] In addition, specialists in cybersecurity visit schools to talk about cybersecurity.[555] In the American University of Malta, you can get a Master's degree in cybersecurity.[556] Several companies in Malta offer cybersecurity training to adults.[557] The B SECURE project has arranged courses in cybersecurity to companies and CSIRT Malta offers cybersecurity training to its members.[558]

The eSkills Malta Foundation, established in 2014 by the Government of Malta, promotes citizens' digital skills and develops the IT sector in Malta. With its partners, it implements various projects to strengthen digital skills. For example, women and senior citizens are offered targeted training to improve digital inclusion. The eSkills Malta Foundation arranges different events, visits schools, publishes studies and provides recommendations to decision-makers. The agenda also includes cybersecurity issues. In 2020, the eSkills Malta Foundation and ĠEMMA, a financial portal, started to cooperate and produce materials depicting the risks of fraud and scams. In 2021, the eSkills Malta Foundation arranged several Digital Skills Bootcamps for various target groups and financed different training courses in digital skills.[559,560]

BeSmartOnline! has operated as Malta's Safer Internet Centre (SIC) since 2010, and it is part of the Insafe, INHOPE and Better Internet for Kids networks supported by the European Commission. The BeSmartOnline! project is coordinated by the Foundation for Social Welfare Services (FSWS), and the participants include the Office of the Commissioner for Children, DLAP and the Cyber Crime Unit of the Malta Police Force. This consortium is supported by several strategic partners who are members of the project's Advisory Board. BeSmartOnline! aims to promote the safe use of the internet and technologies. Its main target group is children and adolescents. Malta's SIC produces various educational materials, articles and news. Its Facebook page shares information about topical events and campaigns, for example. BeSmartOnline! often has a prominent presence at different events, such as fairs.[561,562]

The role of the Cyber Crime Unit of the Malta Police Force is to investigate and prevent crime where a computer is the target, or the means used. It regularly visits schools, youth organisations and different events. The aim is to promote responsible internet use and provide tips on how to best protect against cybercrime. The Police Force website provides citizens with tips on safe internet use.[563]

In 2021, MITA implemented a digital security campaign for seniors. The campaign received prominent coverage in the media and social media, and the face of the campaign was Narcy Calamatta, a popular Maltese actor.[564] Targeted workshops for seniors have been arranged around Malta and Gozo to discuss cybersecurity and various ways to act safely on the internet. A seven-part video series "Digital Age" was also produced to help seniors safeguard their digital security.[565]

Malta has performed well in the DESI comparison but there is room for improvement in the citizens' cybersecurity competencies. A focused project serving all age groups is required to improve the competencies.[566] According to Farrugia (2020), VR games could be produced for children to help them learn how to manage risks associated with the internet in a safe environment. Platforms using AI could be used to teach media literacy. AI could help to identify the users' needs and offer optimal content for each user. Teaching materials should be published both in English and Maltese.[567]

3.14.3. National characteristics

In her Doctoral dissertation (2020), Lorleen Farrugia studied the perceptions of 9–12-year-old Maltese children on online risks and how these perceptions affected their online behaviour. Four out of five children who participated in the study did not view the internet as a safe place. Risks related to technical security, i.e. hacking and viruses, were considered the most dangerous. Three out of four children had faced risks on the internet, the most common of which were viruses and pop-up windows. In these situations, many children had asked for support from their parents, for example. More than 20 per cent of the children in the study did not have any cybersecurity competencies or use any safety measures. According to the study results, multifaceted and versatile collaboration is required to protect children against online risks. Teaching in Maltese schools should be updated. The skills of parents and especially educators should be improved.[568]

3.14.4. The definition of cyber citizen skills

At least basic digital skills are required for citizens to be able to operate in a digital environment. Basic skills include use of hardware and software as well as basic functions on the internet, including cybersecurity competencies.[569] Malta Cyber Security Strategy 2016 encourages citizens to follow at least basic cyber hygiene practices. Examples of related skills include careful handling and sharing online of personal data, installing software updates and antivirus software as well as learning basic security measures, such as the use of strong passwords. Everyone should also be alert for any suspicious actions related to their online accounts.[570]

References

[544] Government of Malta, MITA, *National Cyber Security Strategy 2023-2026* (2022).
[545] Ministry for Competitiveness and Digital Maritime and Services Economy, MITA, *Malta Cyber Security Strategy* (2016.)
[546] Government of Malta, eSkills Malta Foundation, *National eSkills Strategy 2022-2025* (2022).
[547] Government of Malta, eSkills Malta Foundation, *National eSkills Strategy 2019–2021* (2018).
[548] ENISA, *Raising Awareness of Cybersecurity. A Key Element of National Cybersecurity Strategies*, 2021.
[549] "Launch of the NCC and Community," *NCC*, accessed on November 10, 2022. https://ncc-mita.gov.mt/news/launch-of-the-ncc-and-community/.
[550] "NCC Cybersecurity National Coordination Centre Malta," *NCC*, accessed on November 10, 2022. https://ncc-mita.gov.mt/.
[551]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 23–58.
[552] Ministry of Education and Employment, *A National Curriculum Framework for All*, 2012, 37.
[553] A personal communication to the researcher, 08/08/2022.
[554] A personal communication to the researcher, 08/08/2022.
[555] A personal communication to the researcher, 02/09/2022.
[556] "Master of Science in Cyber Security," *AUM American University of Malta*, accessed on 10 November, https://aum.edu.mt/programs/graduate-program-2/cyber-security/.
[557] A personal communication to the researcher, 02/09/2022.
[558] Jason R.C. Nurse, Konstantinos Adamos, Athanasios Grammatopoulos and Fabio Di Franco, *Addressing the EU Cybersecurity Skills Shortage and Gap Through Higher Education*, ENISA (2021), 30.
[559] eSkills Malta Foundation, *Annual Report 2021* (2022).
[560] "ĠEMMA, know, plan, act," *eSkills Malta Foundation*, accessed on September 6, 2022. https://eskills.org.mt/en/gemma/Pages/GEMMA.aspx.
[561] "Maltese Safer Internet Centre," *Better Internet for Kids*, accessed on November 22, 2022. https://www.betterinternetforkids.eu/sic/malta.
[562] "BeSmartOnline!," accessed on September 6, 2022. https://www.besmartonline.org.mt.
[563] "Cyber Crime Unit," *The Malta Police Force*, accessed on September 12, 2022. https://pulizija.gov.mt/en/police-force/police-sections/Pages/Cyber-Crime-Unit.aspx.
[564] "MITA announces a new initiative to help seniors in the digital world," *NCC*, accessed on November 22, 2022. https://ncc-mita.gov.mt/articles/mita-announces-a-new-initiative-to-help-seniors-in-the-digital-world/.
[565] "Cyber Security Malta," accessed on September 6, 2022. https://cybersecurity.gov.mt/.
[566] A personal communication to the researcher, 02/09/2022.
[567] Lorleen Farrugia, *Children and New Media. A Psychosocial Approach to Understanding how Preadolescents Make Sense of Online Risks*, University of Malta: Department of Psychology (2020), 292–293.
[568] Lorleen Farrugia, *Children and New Media. A Psychosocial Approach to Understanding how Preadolescents Make Sense of Online Risks*, University of Malta: Department of Psychology (2020).
[569] Government of Malta, eSkills Malta Foundation, *National eSkills Strategy 2022–2025* (2022), 32.
[570] Ministry for Competitiveness and Digital Maritime and Services Economy, MITA, *Malta Cyber Security Strategy* (2016), 26.

3.15. Portugal

ITU, Global Cybersecurity Index (GCI) 2020	14/182 (Global), 8/46 (Europe)
National Cyber Security Index (NCSI) 2022	8/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	15/27

3.15.1. Strategic cyber education and training policies

Portugal's National Strategy for Cyberspace Security 2019-2023, which also applies to the autonomous regions the Azores and Madeira[571], emphasises prevention, education and increasing awareness. Citizens' digital competencies are improved by the National Digital Skills Initiative e.2030 — INCoDe.2030 programme. Awareness is strengthened and tools are created for the safe and responsible use of digital technologies, giving particular importance to children, adolescents, senior population and other groups at risk. Robust and cross-cutting cybersecurity training programs for organisations and the average citizen is promoted. Cyberspace security skills and knowledge are strengthened by including such themes in the curriculum of primary, secondary and tertiary education and in continuing teacher training. The trust and use of new technology digital resources by new generations (especially vulnerable groups) is promoted in a conscious, informed and responsible manner. Young talents are identified and encouraged to enter the cybersecurity field. Further training in the field is increased and cybersecurity training and requalification courses are certified. Awareness is promoted through awareness campaigns with public and private institutions.[572] According to the strategy, cybersecurity is a shared responsibility between various actors, whether public or private, collective or individual.[573]

The INCoDe.2030 programme[574] is a political initiative to improve digital skills and strengthen Portugal's status and competitiveness. Life is increasingly based on digital technology, and it is important that everyone is equipped to process this new reality. The concept of digital skills is covered extensively in Portugal's INCoDe.2030 initiative. These skills include the concept of digital literacy (the ability to use digital media and technology, critical evaluation of content and efficient communication) and the ability to produce new information through research. This calls for data processing, communication, interaction and producing digital content. The skills can be developed at various levels and using different goals. These different levels are reflected in the type of measures that will be promoted in an inclusive and comprehensive way for the whole of society.[575]

3.15.2. The current state of cyber citizen skills education and training

Cybersecurity education in general (teaching included in the curricula, and for society and citizens) is more focused on security related to internet use and etiquette (*"More security than defence"* perspective) than the security of internet itself. Awareness campaigns cover cybersecurity in general, but they focus on user security and how to react to cyberbullying, for example.[576] In Portugal, informatics (ICT) is taught first as part of other subjects in lower secondary education and later as a separate subject. In primary education in Portugal, teaching is focused on digital skills as part of different subjects. In lower secondary education, informatics is mandatory and integrated into other subjects. One competence area is security. In upper secondary education, it is offered as an optional separate subject. Another competence area is awareness and the power to influence. The subject emphasises advancing technology and its effect on society and everyday life.[577] The Ministry of Education and Portugal's Centre for Cybersecurity coordinate the content of the "Secure Internet" entity in the curriculum of primary and lower secondary education. The aim is to integrate this study module in the content of an existing subject.[578] Portugal's national curriculum has been updated in 2018. With the update, ICT education was

extended to 10–15-year-old pupils, when previously it was only taught to 12–14-year-old pupils. The studies include the above (cyber)security competence area. The teaching content varies at different levels of education. It includes, for example, copyrights, secure digital practices, considerate and respectful attitude, secure online behaviour, falsified email and spam, inappropriate use of images and videos as well as a critical attitude.[579] According to ENISA's CyberHEAD database, cybersecurity is taught in eight different programmes in Portuguese higher education institutions.[580]

Portugal's Safer Internet Centre (PT SIC) belongs to the EU's Better Internet for Kids (BIK) programme, the Insafe awareness centre and the INHOPE hotline network. The PT SIC consortium includes six organisations, such as the Directorate-General for Education (Direção-Geral da Educação, DGE), the Portuguese Institute of Sports and Youth (Instituto Portugês do Desporto e Juventude, IPDJ) and the Altice Foundation (Altice is Portugal's largest telecommunications service provider). The seventh member is the National Cybersecurity Centre (Centro Nacional de Cibersegurança, CNCS), which coordinates and oversees the implementation of the project. PT SIC has two awareness centres. The first one, Centro Internet Segura[581] (SIC), increases awareness and educates the general public. It is managed by CNCS. The second one, the SeguraNet[582] Awareness Centre, is coordinated by DGE. It aims to promote digital citizenship in the school community and raise awareness of online safety (among children, parents, teachers). The centre promotes training for teachers, shares awareness and educational materials, and runs campaigns. DGE also promotes the national plan against bullying and cyberbullying and the Digital Leaders project.[583,584,585] BIK's Safer Internet Day (SID) celebrated in February is celebrated for the entire month in Portugal.[586]

Portugal's National Cyber Security Centre (NCSC) has developed four online courses for citizens: 1) Cybersocial Citizen; secure use of social media (best practices), 2) Cyber-informed Citizen; false news and the risks of uncritical use of information, 3) Cybersafe Citizen; good cyber hygiene practices at leisure and at work (web browsing, protecting the hardware and privacy, responsibility), and 4) Cybersafe Consumer; identifying secure online stores, secure paying and customers' rights in the EU.[587,588] This course package is also offered to public administration, organisations and IT professionals.[589]

The "Digital Academy for Parents" programme is a joint project of DGE and E-REDES in which parents and guardians can participate in the basic digital skills education for children and adolescents.[590] It aims to provide families with basic digital skills to facilitate the monitoring of children's performance in school. In the first part of the programme, teaching focuses primarily on the areas of intervention. The second part also covers security issues (Digital security and citizenship) and the third part also includes a section called Digital consumer.[591,592] IDJP has a national awareness campaign called Naveg@s em Segurança. The campaign promotes secure internet use and digital citizenship. The target groups include children and adolescents, educators, schools, seniors and citizens in general. Included topics cover disinformation, cyberbullying, IoT, online dependency, protection of information, hate speech and social networks.[593] The Portuguese Safer Internet Centre (PT SIC) and the publishing house Pato Lógico developed an image series to raise awareness based on the Zig Zaga na Net podcast. It included a collection of 30 different short stories that were printed as a book. 9,500 of these books were sent to kindergartens, primary education institutions and school libraries in Portugal and the islands.[594,595]The CNCS and the Portuguese Association of Psychologists have an awareness campaign called "What does the internet say about you?"[596] One of the slogans, "Strong passwords and chicken broth never hurt anyone", is aimed at senior citizens. Popular TV presenters Júlio Isidro and Júlia Pinheiro act as the faces of the campaign.[597] DGE's "Cibersegurança nas Escolas" (cybersecurity in schools) is ECSM's extensive campaign in Portugal in 2022 which appeals to all schools to campaign and promote cybersecurity.[598] The campaign material bank contains material for different ages and a book called "Guía para uma Internet segura" (A guide to secure internet).[599]

"The content and offered courses are mainly in Portuguese. Game industry has not yet produced a significant amount of content."[600] Portugal's SIC and the "Eu e os Outros" (Me and the others) programme of SICAD (General-Directorate for Intervention on Addictive Behaviors and Dependencies) developed a video game about

problematic internet use and cybersex. The game is piloted in the schools of the Odivelas Municipality.[601] A media-educational pedagogical quiz "Verdade ou Mentira" (True or false) was developed with journalist Pauolo Pena to promote critical thinking.[602]

Portugal's European Cyber Security campaign for 2021 paid particular attention to the best practices of cyber hygiene using an approachable social media campaign called "In the cybersecurity month, popular wisdom might help". The campaign linked what people know (popular wisdom in the form of proverbs) with what they must learn (cyber hygiene practices). Traditional Portuguese tiles serve as a graphical background for the content (for example "Laziness is the mother of all evil". TURN ON TWO-FACTOR IDENTIFACTION WHENEVER POSSIBLE.) The traditional Portuguese tiles [603] emphasised the popular and traditional elements of the messages to all generations. Some of the proverbs were engraved on physical tiles and given out at CNCS' annual C-Days Conference.[604]

3.15.3. National characteristics

The cybersecurity culture in Portugal is framed by ethical principles under which it is ensured that everyone has sufficient information and awareness and is confident in using information networks and systems.[605] In Portugal, cybersecurity is based on the role of the citizens. Everyone plays a role in cybersecurity and is responsible for protecting themselves and others.[606] Participating in cybersecurity and its promotion is considered important.[607] Developing citizens' digital skills creates resilience in Portugal, making it a more resilient society[608].

In Portugal, digital citizenship is also addressed in three projects related to school communities. The concept of "Cidadania Digital" (Digital citizenship) entails the above SeguraNet programme and its projects called "Líderes Digitais" (Digital Leaders) and "Selo de Segurança Digital" (eSafety ID).[609] The aim of the Digital Leaders project is to improve media literacy of pupils of the same age and the school community and increase secure and conscious internet use. It also aims to facilitate the development of digital citizenship. Pupils arrange unofficial training sessions in their own school community.[610,611] The European eSafety project is aimed at all schools with the goal of promoting and certifying the digital security practices in schools.[612]

3.15.4. The definition of cyber citizen skills

At its simplest, e-citizenship means good behaviour in the digital world, but it entails a lot more. It covers digital etiquette, communication, security and legislation, access and inclusion, digital skills, rights and obligations and participation.[613] In Portugal, cyber citizen skills emphasise secure internet use and security issues related to etiquette and user safety (for example how to react to cyberbullying) (*"More security than defence" perspective*).[614]

In Portugal, the dynamic framework for digital competence (Quadro Dinâmico de Referência de Competência Digital, QDRCD) is based on the Digital Competence Framework for Citizens. It has five fields of expertise: 1) Information literacy, 2) communication and citizenship, 3) content creation, 4) security and privacy, and 5) development of solutions. The skills levels vary from basic to very advanced. The communication and citizenship field of expertise includes citizenship through digital technologies, code of conduct in a digital environment and digital identity management. The security and privacy field of expertise includes device protection, personal data protection as well as health and environment protection.[615] In Portugal, cyber citizen skills can also be defined by the above four online courses offered by NCSC and their content.[616] The aim is also to develop digital citizenship in the school world by raising trusting citizens who are able to meet digital challenges in a safe and responsible manner.[617]

References

[571] A personal communication to the researcher, 03/10/2022.
[572] Resolution of the Council of Ministers No. 92/2019, *Portugal National Strategy for Cyberspace Security 2019-2023*, *Portuguese Official Journal*, Series 1 – No. 108 (5 June 2019), 2,891–2,892.
[573] Council of Ministers, *Strategy for Cyberspace Security*, 2889.
[574] "Portugal INCoDe.2030, The Programme," accessed on 30 November 2022, https://www.incode2030.gov.pt/en/programme.
[575] "A INCoDe.2030," accessed on October 11, 2022. https://www.incode2030.gov.pt/en/initiative.
[576] A personal communication to the researcher, 03/10/2022.
[577] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 10-62.
[578] A personal communication to the researcher, 03/10/2022.
[579] Global Forum on Cyber Expertise (GFCE), *Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people*, Krysia Emily Waldock, Vince Miller, Shujun Li and Virginia N.L. Franqueira Institute of Cyber Security for Society (iCSS) (UK: University of Kent, February 2022), 98.
[580] "CYBERHEAD – Cybersecurity Higher Education Database," *ENISA*, accessed on 22 November 2022, https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=prt.
[581] "Centro Internet Segura," accessed on November 30, 2022. https://www.internetsegura.pt/.
[582] "SeguraNet, Navegar em Segurança," accessed on November 30, 2022. https://www.seguranet.pt/.
[583] Portuguese Safer Internet Centre V, Centro Internet Segura, *Final Public Report, January 1st, 2020 – December 31th* (2020), 13–14.
[584] "Portuguese Safer Internet Centre," accessed on November 21, 2022. https://www.betterinternetforkids.eu/sic/portugal.
[585] "Portuguese Safer Internet Centre, About us," accessed on November 21, 2022. https://www.saferinternetday.org/in-your-country/portugal.
[586] "Portuguese Safer Internet Centre, About our SID activities," accessed on November 21, 2022. https://www.saferinternetday.org/in-your-country/portugal.
[587] A personal communication to the researcher, 12/07/2022.
[588] "E-learning Courses," accessed on November 22, 2022. https://www.cncs.gov.pt/en/e-learning/.
[589] "E-learning Courses>Public Administration/ Organizations/ IT Professionals," accessed on November 22, 2022. https://www.cncs.gov.pt/en/e-learning/.
[590] A personal communication to the researcher, 12/07/2022.
[591] "Academia Digital para Pais (3.ª Edição)," accessed on November 23, 2022. https://www.dge.mec.pt/academia-digital-para-pais-3a-edicao.
[592] "Investimento social, Conheça os nossos programas, Um projeto de literacia digita," accessed on November 23, 2022. https://www.e-redes.pt/pt-pt/sustentabilidade/nos-e-as-comunidades/investimento-social/academia-digital-para-pais.
[593] "Programa «Naveg@s em Segurança?» - sessões de sensibilização de Cidadania Digital," accessed on November 23, 2022. https://erte.dge.mec.pt/noticias/programa-navegs-em-seguranca-sessoes-de-sensibilizacao-de-cidadania-digital-0.
[594] "ZigZaga on the Internet," accessed on November 30, 2022. https://cybersecuritymonth.eu/countries/portugal/zigzaga-on-the-internet.
[595] A personal communication to the researcher, 12/07/2022.
[596] "O que a Internet diz de si!," accessed on November 30, 2022. https://www.internetsegura.pt/o-que-internet-diz-de-si.
[597] "New awareness-raising campaign for senior users," accessed on 23 November 2022, https://www.betterinternetforkids.eu/practice/articles/article?id=6918638.
[598] "Cibersegurança nas Escolas," accessed on November 23, 2022. https://cybersecuritymonth.eu/countries/portugal/ciberseguranca-nas-escolas.
[599] "CIBERSEGURANçA NAS ESCOLAS, Recursos de Apoio," accessed on November 24, 2022. https://www.seguranet.pt/mes-ciberseguranca-2022/recursos-de-apoio.
[600] A personal communication to the researcher, 03/10/2022.
[601] A personal communication to the researcher, 12/07/2022 and 18/07/2022.
[602] "Jogo Pedagógico Verdade ou Mentira," accessed on November 24, 2022. https://www.seguranet.pt/pt/jogo-pedagogico-verdade-ou-mentira.
[603] "MÊS EUROPEU DA CIBERSEGURANÇA, A SABEDORIA POPULAR PODE AJUDAR," accessed on November 30, 2022. https://www.cncs.gov.pt/docs/1626333366.pdf.
[604] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 121–126.
[605] Council of Ministers, *Strategy for Cyberspace Security*, 2891.
[606] "Citizen," accessed on November 20, 2022. https://www.cncs.gov.pt/en/citizen/?persona=citizen.
[607] Portuguese Safer Internet Centre V, Centro Internet Segura, *Final Public Report, January 1st, 2020 – December 31th* (2020), 2.
[608] Council of Ministers, *Strategy for Cyberspace Security*, 2891.
[609] "Equipa de Recursos e Tecnologias Educativas >CIDADANIA DIGITAL," accessed on November 21, 2022. https://erte.dge.mec.pt/noticias/programa-navegs-em-seguranca-sessoes-de-sensibilizacao-de-cidadania-digital-0.
[610] A personal communication to the researcher, 12/07/2022.
[611] "Líderes Digitais SeguraNet," accessed on November 21, 2022. https://www.seguranet.pt/pt/lideres-digitais-seguranet.
[612] "eSafety Label (Selo de Segurança Digital)," accessed on November 22, 2022. https://erte.dge.mec.pt/esafety-label.
[613] "A Internet pode favorecer a cidadania?," accessed on November 18, 2022. https://mild.rbe.mec.pt/a-internet-pode-favorecer-a-cidadania/.
[614] A personal communication to the researcher, 03/10/2022.
[615] "INCODE.2030 Digital Competence Reference Framework," accessed on October 20, 2022. https://www.incode2030.gov.pt/en/featured/incode2030-releases-digital-competence-dynamic-reference-framework.

[616] "E-learning Courses," accessed on November 24, 2022. https://www.cncs.gov.pt/en/e-learning/.
[617] "O que fazemos?," accessed on November 21, 2022. https://www.seguranet.pt/pt/o-que-fazemos.

3.16. Poland

ITU, Global Cybersecurity Index (GCI) 2020	30/182 (Global), 18/46 (Europe)
National Cyber Security Index (NCSI) 24 October 2022	10/160 (24 October 2022)
The Digital Economy and Society Index (DESI, 2022)	24/26

3.16.1. Strategic cyber education and training policies

Andrzej Duda, the President of Poland, approved the new National Security Strategy of the Republic of Poland in May 2020. One of the key elements of the strategy is cybersecurity. The strategy is Poland's most important national document. One of the related strategies is the Cybersecurity Strategy of the Republic of Poland for 2019–2024. One important objective is to increase measures to allow citizens to better protect their information. According to the strategy, cybersecurity training should be started as early as possible, even before access to digital services. In practice, training should be started in early childhood education. Higher education institutions are encouraged to develop multi-disciplinary programmes which cover information security. The strategy also takes into account educational activities and campaigns for citizens which aim to increase general awareness. These are implemented for different target groups, such as children, adults and seniors.[618]

The National Framework of Cybersecurity Policy of the Republic of Poland includes proposed special measures for the field of education. The framework covers years 2017–2022. The National Framework emphasises development of interdisciplinary expertise, development of new technology in Polish universities and improving the competence of IT teachers. According to the framework, safe use of cyberspace must be part of the curriculum, at the early stage of education. The framework also aims to target cybersecurity campaigns to different groups (children, parents, seniors).[619]

3.16.2. The current state of cyber citizen skills education and training

The basic education curriculum adopted in 2017 and the mainstream education curriculum mention cybersecurity as part of security training. The aim is to initiate measures for pupils in primary school, lower secondary school and upper secondary school to share information about cybersecurity, create a critical attitude towards Internet content and promote secure online behaviour. Some upper secondary schools also offer the opportunity to specialise in cybersecurity. The aim is also to initiate collaboration between educational and private operators in various educational projects, joint projects or workshops. In general, it has been stated in Poland that measures to develop the digital skills of kindergarten children should be targeted to their parents. A digitally competent parent is able to support the child's development in cooperation with early childhood education. In principle, upbringing should include development of computational thinking, media education, different class scenarios and didactic tools adapted to pre-schoolers.[620]

Cybersecurity training is offered to higher education students as part of the Legia Akademicka programme, but Legia Akademicka prepares students for taking the military oath. The aim is to train and recruit more professionals. Citizens are also offered the opportunity to serve in the Territorial Defence Forces, which is similar to the National Defence Training Association of Finland (MPK). The Territorial Defence Forces are called the WOT forces. The WOT forces also have a cyber unit. Members of the forces are offered regular training and practice along with working life. In addition, the Academy of Military Art offers cybersecurity and information security events which are also open for citizens.[621]

Polish universities arrange education related to cybersecurity. Degree programmes are offered subject to a fee and degree studies free of charge. Generally, the content is focused on improving technical competence. The term cybersecurity is included in the name of the following degree programmes: Cybersecurity - Akademia Ignatianum in Krakow, Cybersecurity – AGH University of Science and Technology, Cybersecurity (IT Cyber Security) - Maria Curie-Skłodowska University in Lublin, Information security and cybersecurity - Academy of War Arts in Warsaw, Cybersecurity - Wroclaw University of Science and Technology and Cryptology and cybersecurity - Military University of Technology Jarosław Dąbrowski in Warsaw.[622]

Together with the Class Foundation, Polish primary education schools arrange an education programme called "Asy Internetu" (Be Internet Awesome) which aims to teach citizens how to be good people on the Internet. The programme is based on following universal principles both in the real world and the digital world. These principles include sensibility, awareness, strength, friendliness and courage. The programme includes dozens of class scenarios to be used in the classroom and in remote learning. The lessons focus on sharing and evaluating information, recognising various online scams and protecting yourself by using strong identification, for example.[623]

In addition to the central government, there are several operators in Poland who promote the development of citizens' cyber awareness and competence. The most important operator is the National Research Institute (NASK), operated under the Prime Minister's Office. NASK's tasks include managing Poland's national education network, responsibility for the national register of domain names and studying the social implications of digitalisation. NASK arranges cybersecurity training for citizens and organises different information campaigns annually. One example of this is a guidance for schools "Online safety in the schools of the Polish educational Network". As part of Poland's national educational network, it has created a free mOchrona application which supports parents in keeping their children safe online. NASK has also entered into national agreements with key non-governmental organisations to strengthen cooperation with the aim of increasing awareness of cybersecurity.[624] Some platforms for practising cyber skills have been developed for citizens but they are mainly targeted to users who want to deepen their knowledge and companies that want to purchase training for their employees. The offered training is subject to a fee. Related websites include: ZaufanaTrzeciaStrona.pl, Niebezpiecznik.pl, Sekurak.pl and CyberDefence24.pl.[625]

OSE IT School is an educational platform that offers access to free online education materials and courses. The platform is especially aimed at students, but also at teachers. It offers more than 200 free courses, and users can plan their own educational path. The platform also considers different age groups.[626] NASK maintains a website called European Cybersecurity Month (ECSM). In 2022, this campaign was implemented in Poland for the eight time. The website is the home page for this month-long campaign, but it also includes a significant amount of related material to improve awareness and learning.[627] The Digital Poland of Equal Opportunities programme (PCRS), a joint project of the Ministry of Administration and Digitization and the Cities On Internet Association, is an initiative aiming to encourage people over 50 to take a first step into the digital world.[628] The "Cities on the Internet" project was targeted at people over 50, and it was implemented in 2016–2018. The aim of the project was to develop digital competence, and the participants decided the topics to be addressed. The project was continued, and now a similar project will be implemented to teach cyber skills for people over 18.[629] The Polish Safer Internet Centre (PSIC) was established in 2005 under the Safer Internet programme of the European Commission, and now it operates under the Digital Europe programme. The centre consists of NASK (PSIC's coordinator) and the Empowering Children Foundation (ECF). The centre implements extensive measures to ensure the safety of children and adolescents using the Internet and new technology. Its target groups include children, adolescents, parents, teachers and other professionals working to protect children from the dangers of the Internet. The centre arranges conferences and produces educational material and social campaigns. The centre also organises the annual Safer Internet Day which has been celebrated since 2005.[630]

The Sieciaki.pl "get to know safe internet" website is intended for 6–12-year-old children. It addresses safe Internet use through games, comics and books.[631] The Necio website is intended for 4–6-year-old children and

their parents. The website talks about Internet and what happens on the Internet using videos, exercises and comics in an interactive manner.[632] The Protect your child online campaign aims to warn parents about the consequences of harmful exposure of pre-schoolers and children in early grades to the Internet and show how to reduce the risk of harmful contacts. The campaign is arranged by the Empowering Children Foundation (former Nobody's Children Foundation) and NASK as part of the operation of the Polish Safer Internet Center.[633]

“Rufus in peril” is an educational game that shows what kind of dangers a young user of modern technology faces and how to react in difficult situations. Its graphical design and language have been adapted to players in primary and lower secondary school, but older users of modern technology may also find it contains something interesting.[634]

Conferences on cybersecurity are also arranged for teachers and head teachers on a local level. These are arranged especially by the schools’ local education committees and education centres. For example, the Board of Education in Rzeszow arranges an Online Conference: Cybersecurity at School.[635] NASK organises courses on cybersecurity for teachers. “Safe in the Web with OSE”, NASK’s educational series on cyber threats for teachers, is about to start. In this programme, the instructors receive information about phenomena, such as sexting, cyberbullying or FOMO, helping them to better support the pupils to cope with the cyber threats and challenges brought by distance learning.

The e-learning portal is a digital platform solution for teachers and students. It introduces various areas and technologies related to cybersecurity, such as AI, algorithms, programming, databases, chemistry, physics and multimedia. The platform can be used to produce campaigns and competitions for various purposes.[636]

3.16.3. National characteristics

TrendMicro Poland has created a Cybersecurity Education for Universities programme to support colleges in arranging cybersecurity programmes free of charge. Together with schools, TrendMicro arranges seminars and webinars for students to offer the latest expert information. TrendMicro also consults education programmes to ensure that the subjects in the curriculum correspond to actual needs and enable quick access to relevant information in the changing world of technology and cybercrime.[637]

3.16.4. The definition of cyber citizen skills

In Poland, citizens’ cybersecurity competence is not defined on a national level. Based on the received responses, citizens are mainly instructed to view information found on the Internet critically. According to experts, the definition of these skills is still in its infancy. This is also reflected in the act of 2018 on cybersecurity systems. According to this act, cybersecurity can be viewed as a counterforce for activities which violate the confidentiality, integrity, accessibility and authenticity of information offered by cybersecurity systems or related services. This definition could be interpreted to have a strong emphasis on information security. A special delegate has been appointed to the Government to oversee information security.[638]

References

[618] Ministry of Digital Affairs, *Cybersecurity Strategy of the Republic of Poland for 2019–2024* (2019), 10, 26; A personal communication to the researcher, 23/08/2022.
[619] A personal communication to the researcher, 25/08/2022.
[620] Chancellery of the Prime Minister, *Digital Competences development program* (2022), 24–26, 57–59, 60–64; A personal communication to the researcher, 21/10/2022.
[621] A personal communication to the researcher on 21/10/2022, "Dowództwo Wojsk Obrony Terytorialnej," accessed on October 12, 2022. https://terytorialsi.wp.mil.pl/.
[622] "Studia cyberbezpieczeństwa," *Studia.pl*, accessed on 20 October 2022, https://studia.pl/kierunki/cyberbezpieczenstwo/; "Education," *AGH*, accessed on September 12, 2022. https://iet.agh.edu.pl/en/education/.
[623] "Asy Internetu," accessed on October 16, 2022. https://asyinternetu.szkolazklasa.org.pl/wez-udzial/.
[624] "NASK," accessed on September 23, 2022. https://www.nask.pl/; "NASK," accessed on 11 August 2022, https://www.nask.pl/pl/aktualnosci/3795,Cyberbezpieczny-uczen-cyberbezpieczna-szkolaporadniki-dla-szkol-o-bezpieczenstw.html?search=60470; A personal communication to the researcher, 10/08/2022.
[625] A personal communication to the researcher, 15/08/2022 and 20/08/2022.
[626] "OSE IT Szkoła," accessed on November 10, 2022. https://it-szkola.edu.pl/.
[627] "Europejski Miesiąc Cyberbezpieczeństwa," *NASK*, accessed on 18 September 2022, https://bezpiecznymiesiac.pl/.
[628] "National Digital Literacy Campaign," *Polska Cyfrowa Rownych Szans*, accessed on 2 September 2022, https://latarnicy.pl/english/.
[629] A personal communication to the researcher, 24/08/2022.
[630] A personal communication to the researcher, 09/08/2022.
[631] "Sieciaki.pl," accessed on October 2, 2022. https://sieciaki.pl/.
[632] "Necio.pl," accessed on September 20, 2022. https://www.necio.pl/.
[633] "Chroń dziecko w sieci," accessed on September 13, 2022. http://www.dzieckowsieci.pl/kampania/; Joanna Świątkowska, Izabela Albrycht and Dominik Skokowski, *National Cyber Security Organization: POLAND* (Tallinn: CCDCOE, 2017).

[635] "Konferencja on-line: Cyberbezpieczeństwo w szkole," *Kuratorium Oświaty w Rzeszowie*, accessed on June 22, 2022. https://www.ko.rzeszow.pl/dla-dyrektora-i-nauczyciela/dla-dyrektora-i-nauczyciela-komunikaty/konferencja-on-line-cyberbezpieczenstwo-w-szkole/.
[636] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022).
[637] Kancelaria Sejmu, *O krajowym systemie cyberbezpieczeństwa*, *Dz. U. 2018 poz. 1560*, accessed on August 21, 2022. https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf; A personal communication to the researcher, 21/11/2022.
[638] "Edukacja z zakresu cyberbezpieczeństwa dla uniwersytetów," *TrendMicro*. Accessed on October 8, 2022. https://www.trendmicro.com/pl_pl/initiative-education/cybersecurity-education-universities.html.

3.17. France

ITU, Global Cybersecurity Index (GCI) 2020	9/182 (Global), 5/46 (Europe)
National Cyber Security Index (NCSI) 2022	13/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	12/27

3.17.1. Strategic cyber education and training policies

In 2008, Nicolas Sarkozy, the president of France, decided that due to the changed cybersecurity situation, France should prepare a white paper on defence and national security. The aim of the white paper was to define the threats and risk factors affecting the nation as well as measures to control them.[639] With regard to cybersecurity, this white paper has been characterised as pivotal and the first strategy on the state level to recognise the significance of cyber threats. In 2013, a new white paper on defence and national security was prepared at the request of President François Hollande. The strategic goals described in the white paper led to the establishment of the French National Agency for the Security of Information Systems (Agence nationale de la sécurité des systèmes d'information, ANSSI). ANSSI operates under the General Secretariat for Defence and National Security (Secrétariat général de la défense et de la sécurité nationale, SGDSN) under the French Prime Minister.[640]

One of the tasks assigned to ANSSI was to prepare a national cybersecurity strategy, which was published in 2011 and updated in 2015. The aim of the updated national cybersecurity strategy was to guide France's transition towards a digitalising society, and it included five strategic objectives. The third objective was to improve the awareness on digital security and responsible behaviour in the cyber world among school children. According to the strategy, a study module on digital security should be added to tertiary education and further education. Its aim is to improve citizens' competence by integrating cybersecurity training in all tertiary education and continuing education programmes.[641]

The objective of the national cybersecurity strategy according to which France intends to protect the use of digital services by citizens and strengthen the prevention of cybercrime and providing help to its victims, led to the establishment of an aid system called GIP ACYMA (Le Groupement d'Intérêt Public Action contre la Cybermalveillance) in November 2017. The system aims to aid and support citizens exposed to cyber attacks, such as private individuals, companies and operators in the public sector, and to prevent incidents by raising awareness on the topic. In 2022, ACYMA has approximately fifty members from the private and public sector.[642]

The White Paper on Defence and National Security published in 2013 brings up the impact of increasing the number of information security and cybersecurity experts trained in France on national security. According to the white paper, it should also be ensured that information security and cybersecurity have been integrated into university degrees in computer science to prevent creation of information system vulnerabilities and to promote vigilance and responding to cyber threats. To attain the objectives, ANSSI contributed to the creation of the CyberEdu programme intended to offer resources for educational institutions arranging the above education. As a result, the CyberEdu association was established. The task of the association is to develop and maintain its original programme and to approve courses offered by educational institutions which fulfil the requirements of the programme. In the autumn 2019, CyberEdu published 78 certified education programmes. Increase in the number of trained information security and cybersecurity experts in France contributed to certain measures initiated by ANSSI, such as the SecNumedu certification for the recognition and promotion of education.[643]

3.17.2. The current state of cyber citizen skills education and training

To make cybersecurity training available also for French citizens, such as school children (in line with the strategy), ANSSI MOOC was established in March 2017. MOOC intends to teach and raise citizens' awareness on challenges related to digital security. MOOC is a browser-based free-of-charge learning environment intended for working users. The offered exercises strengthen competence and focus on the cybersecurity of workplaces and homes. MOOC's target group is citizens who want to learn the basics of digital security and cybersecurity. The training is defined by CFSSI and implemented by the agency's technical experts. The ANSSI MOOC offers fun educational content that is accessible for everyone around the clock.[644] The training is divided into four teaching modules in which you learn the basics of information and digital security and cybersecurity. This information is useful in your daily life, both at home and at work.

In addition to MOOC, France has tried to develop the cybersecurity competence of citizens and especially children and adolescents with the help of Pix, for example. Pix is a French non-profit public organisation, which aims to develop people's digital skills all around the world. Pix was established in 2016 and is backed by approximately 70 experts in various fields who want to help people to improve their digital skills. Pix also cooperates with UNESCO to develop adolescents' digital skills around the world. The international website pix.org has been developed under the UNESCO Youth employment in the Mediterranean (YEM) project funded by the European Union. The Pix.org website contains an online learning platform created for the purpose of evaluating and improving your digital skills.[645]

The learning platform includes a game with different exercises related to the digital world. You can play the game both in French and in English. The game includes different questions and practical exercises related to the creation of passwords, word processing, information search and general knowledge. The game has five areas: information and data, communication and collaboration, content creation, protection and security, and digital environment. According to statistics, approximately 63,000 users play the game daily.

The ANSSI Cybersecurity Training Center (CFSSI) also has a key role in increasing cybersecurity training. CFSSI plays an important role in the definition and implementation of the educational policy concerning the security of national information systems. CFSSI also coordinates a programme called SecNumedu, which aims to ensure that cybersecurity training offered to students and employees, for example, is in line with the agreements determined by ANSSI and operators in the field and meet the criteria.[646]

A process implemented by SecNumedu allows to ensure that the scope and relevance of the education programme's content are in line with the learning goals. The SecNumedu certification was developed in cooperation with companies, higher education institutions, associations and the French Ministry of National Education, and it is awarded for three years at a time. ANSSI is responsible for the certification and maintains a list of certified education programmes. According to ANSSI, there were 72 SecNumedu certified education programmes offered by different educational institutions in 2022. These were mainly vocational qualifications, degrees in engineering and Master's degree programmes.[647] According to ENISA (the European Union Agency for Cybersecurity), there were eleven higher education programmes focused on cybersecurity in France in 2022.[648]

In 2017, ACYMA launched the Cybermalveillance.gouv.fr platform. The platform aims to help the victims of cyberattacks and cybercrime by offering them advice and help. It also intends to raise awareness of digital security with the included information packages. The information packages consist of nine themes which are available in different formats, such as posters, videos or comics. You can also learn about the content of the information packages through a quiz game. The packages contain basic information about good practices in the digital world, such as strong passwords, backups, social media security and the importance of updates. They also offer plenty of topical information about different risks and threats, such as phishing and various malware. The information packages have been created together with ACYMA's members.[649]

Safer Internet France is the French part of the European Better Internet for Kids programme, launched by the European Commission in 2008. The French Safer Internet programme is based on three lines of action: a helpline, a national awareness plan (Internet Without Fear) and a forum where you can report illegal Internet content. Safer Internet Centres (SIC) also organise the annual international Safer Internet Day featuring national events and campaigns. The French SIC has also implemented a programme called FamiNum which teaches families about good and secure practices in the digital world.[650]

3.17.3. National characteristics

Even though France has spoken for years about the importance of effective defensive and offensive approach in cyber warfare, it has also brought up the importance of human factors as part of holistic cybersecurity and seeks to influence this by offering diverse cybersecurity training. Like several other countries, France wants to integrate cybersecurity training in all levels of education, but it also offers training focused on the basics of cybersecurity for citizens. In addition to education, France employs several ways to raise citizens' awareness on cybersecurity and offers support for victims of cybercrime in line with its cyber strategy.

the French National Agency for the Security of Information Systems (ANSSI) is located in the 13-floor Cyber Campus building opened in 2022, in La Defense region, Paris. The Campus is part of President Emmanuel Macron's cybersecurity project to develop cybersecurity in France and allow different operators, such as companies, educational organisations, researchers and associations, to work in the same premises. Cyber Campus also aims to meet the demand for increased training by developing educational activities. The ANSSI Cybersecurity Training Center (CFSSI) is also located in the Cyber Campus.[651]

In addition, France plays an important role as a builder of national and international cybersecurity networks. During the Paris Peace Forum, on 12 November 2018, France initiated the Paris Call for Trust and Security in Cyberspace. The Paris Call for Trust and Security in Cyberspace encourages all operators in cyberspace to commit to protecting the common cyberspace. This Call is the first significant initiative that brings together countries, companies and associations in Europe and around the world.[652]

3.17.4. The definition of cyber citizen skills

France has not defined its cyber skills in detail, but the civic skills can be taken to be based on the content of the educational packages aimed at citizens, which often focus on the basic knowledge and skills required in the digital world. This knowledge and skills enable responsible behaviour in the digital space, improving the security of yourself and others. In France, the teaching of cyber citizen skills is targeted to all citizens and age groups.

References

[639] Philippe Baumard, *Cybersecurity in France* (SpringerLink, 2017), 56; Pascal Brangetto, *National Cyber Security Organisation: France* (Tallinn: CCDCOE, 2015), 8.
[640] "SGDSN in English," *Secrétariat général de la défense et de la sécurité nationale*, accessed on November 30, 2022. http://www.sgdsn.gouv.fr/accueil/sgdsn-in-english/.
[641] République Française, Premier Ministre, *Estrategia Nacional Francesa para la seguridad del ambito digital*.
[642] "Arrêté du 3 mars 2017 portant approbation de la convention constitutive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance. Arrêté du 3 mars 2017 portant approbation de la convention constitu-tive du groupement d'intérêt public pour le dispositif national d'assistance aux victimes d'actes de cybermalveillance – Légifrance," *Legifrance*, accessed on September 25, 2022. www.legifrance.gouv.fr.
[643] Guillaume Poupard, *PROCESSUS POUR L'OBTENTION DU LABEL SECNUMEDU*, Prime Minister (2016).
[644] "SECNUMACADÉMIE," *Agence nationale de la sécurité des systèmes d'informatio*, accessed on September 15, 2022. https://www.ssi.gouv.fr/entreprise/formations/secnumacademie/.
[645] "Cultivez vos compétences numériques," *Pix*, accessed on September 12, 2022. https://pix.org/fr/.
[646] Borka Jerman Blažič, *Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?* (Springer, 2021), 3025.
[647] "FORMATIONS LABELLISÉES SECNUMEDU," *Agence nationale de la sécurité des systèmes d'information*, accessed on October 2, 2022. https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/.
[648] "CYBERHEAD - Cybersecurity Higher Education Database," *ENISA*, accessed on November 30, 2022. https://www.enisa.europa.eu/topics/education/cyberhead#/.
[649] "Assistance aux victimes de cybermalveillance," *Cybermalveillance*, accessed on October 20, 2022. https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/qui-sommes-nous.
[650] "Safer Internet France, Programme national de prévention et d'éducation aux bons usages d'Internet," accessed on November 5, 2022. https://www.saferinternet.fr.
[651] Michel Van Den Berghe, Yann Bonnet, Charly Berthet, Christian Daviot, Jean-Baptiste Demaison and Faustine Saunier, *Cyber Campus, Uniting and expanding the cybersecurity ecosystem* (2021).
[652] "Appel de Paris Pour la confiance et la sécurité dans le cyberspace," *Appel de Paris 12.11.2018*, accessed on November 30, 2022. https://pariscall.international/fr/.

3.18. Romania

ITU, Global Security Index (GCI) 2020	62/182 (Global), 32/46 (Europe)
National Cyber Security Index (NCSI) 2022	7/160 (24 October 2022)
The Digital Economy and Society Index (DESI, 2022)	27/27

3.18.1. Strategic cyber education and training policies

In 2021, the Government of Romania published a new cybersecurity strategy and its implementation programme for 2022–2027. The updated strategy defines new objectives and identifies factors that are important in terms of the functionality of digital services and their secure use. The aim of Romania's national cybersecurity strategy is to create a framework for the future development of central government, business environment, national economy and the education and research field.[653]

The strategy emphasises systematic building and further development of a coherent cybersecurity culture. With regard to the culture, raising citizens' general awareness of protecting the cyberspace and its functionalities and information systems as well as protecting against threats, vulnerabilities and risks has been identified as a key lever. The measures defined in the strategy help Romania to meet the security objectives and commitments of NATO and the European Union. Romania considers it essential to actively participate in international research, cooperation, events and information sharing in the field of cybersecurity.[654]

In Romania, the National Strategy on the Digital Agenda for Romania 2020, prepared in 2015, guides the activities and sets the goals of society for the development of information and communication technologies (ICT) skills. The aim is to create a solid knowledge base and train a professional workforce for the needs of cybersecurity, cloud services, open data, big data and social media related fields. Values and goals that are pivotal for Romanian society, such as fighting the climate change, energy shortfall, poverty and social exclusion, are given special weight in the definition and regulation of different sectors, such as manufacturing, research and development.[655]

In 2022, a cybersecurity directorate (Directoratul Naţional de Securitate Cibernetică, DNSC) was established under the Prime Minister's Office to coordinate cybersecurity issues in the central government. Romania uses a part of the targeted EU recovery funds for the establishment of the directorate and its identified cybersecurity projects. The established directorate serves as a link between public administration, business and academia, aiming to create coherent and resilient cybersecurity architecture at national level. DNSC organises awareness campaigns on topical themes, such as prevention of spam, malware and cybercrime, and informs citizens of the current cyber situation and changes in the threat landscape (CERT-RO). DNSC plays a key role in implementing the new national cybersecurity strategy and ensuring compliance. [656,657]

3.18.2. The current state of cyber citizen skills education and training

From the view of developing cyber citizen skills, Romania's new curriculum addresses the creation and implementation of mandatory education programmes on cybersecurity at different levels of education. Romania's Government invests in the development of educational technology as part of implementing the Digital Education Action Plan 2021–2027 published by the European Commission. Romania has allocated EUR 881 million to digitalisation of education, as part of the country's recovery and resilience plan. The funds will be used for improving digital pedagogical competence, educational content, hardware and other resources based on three principles: i) improving education systems through better data analysis and foresight, ii) making better

use of digital technology for teaching and learning, and iii) developing relevant digital skills and competences for digital transformation. The measures aim to cut down costs related to the public sector and the use of public services and to modernise educational structures. During the Covid-19 pandemic, higher education institutions in Romania have shown a very high capacity to adapt to digital teaching models, but they require additional resources and dedicated training to support this model.[658]

As the DESI index shows, Romania's previous investment in the digital basic training for citizens has been low. As a result, Romania's Government took action to improve the current state of competence and education. Three projects were started in February 2017: Cyber_Education, Cloud_Education and K5-K8 Curricular Reform.[659]

In the Cyber_Education project funded by the European Union, Romania's nine largest universities were invited to create joint and modern curricula for cybersecurity and educational laboratories. The project was launched by the Bucharest University of Economic Studies, which educates experts in cybersecurity.[660] An integral part of the Cyber_Education project is the Cloud_Education programme, which focuses especially on competence building in the area of new technologies, such as cloud services, big data, social media and mobile programming. The K5-K8 Curricular Reform project modernised the curricula for grades 5–8 in Romanian elementary schools (11–14-year-olds) in terms of information technology and computer science. As a result of the project, cybersecurity awareness was included in education programmes and study modules concerning software design, coding, 3D modelling and virtual reality. The new curriculum complies with the principles of Professor Seymour Papert (Massachusetts Institute of Technology). Implementation of cybersecurity and digital skills coaching and training for teachers is ongoing.[661]

Romania has 54 public and 35 private universities in 24 cities, serving more than 550,000 students. Romanian universities specialising in cybersecurity training are Technical University of Cluj-Napoca, Information and Computing System Security, and University Politehnica of Bukharest, Faculty of Applied Sciences, Coding and Storage Theory of Information Master. [662,663,664]

In 2012, the Romanian Association for Information Security Assurance (RAISA), was established under the project. It is a professional, independent, impartial non-profit association. RAISA aims to promote and support society's activities by increasing information exchange between the public, private and academic operators in Romania. The parties must commit to the following values: continuous investment in education, openness to new methods to protect data, participating in the prevention of cybercrime, focusing on facts and fostering excellence. RAISA's vision is to promote research and education in the information security field and contribute to the creation and dissemination of knowledge and technology in this domain. RAISA has a strong representation at national level. It brings together professors and researchers from top universities and Romanian institutions, PhD, Masters and licentiate students, as well as companies from the IT segment. RAISA's motivation is that any company, organisation or community benefits from investing in systems security to prevent security risks when the systems are connected to the Internet.[665]

The Cyber4Kids campaign wants to educate parents and their children about the risks that children are exposed to on the Internet and how to protect yourself against them. The campaign's video animation series explains what cybersecurity means. Each episode has a related guide with Internet security tips. There is one section for parents and another one for children.[666]

MyDigiSkills helps you to better understand your level of digital skills based on knowledge, skills and attitude in each of the five areas of the European Digital Competence Framework for Citizens (DigComp). The website contains 82 questions on digital skills, and you will get a report on your skill level based on your answers. The forum is Europan, but it is also available in Romanian.[667]

Ora de Net is a programme that encourages children and adolescents to use Internet in a creative, useful and secure manner. The programme organises training and develops courses for parents, teachers and experts. Ora

de Net provides advice on any questions related to Internet or online profiles. You can report illegal content found on Romanian websites to Ora de net to help build safer Internet. The programme also coordinates an extensive network of voluntary teachers and experts. The volunteers work with children and implement educational activities on a national level.[668]

Fundația EOS – Educating for an Open Society (EOS Romania – www.eos.ro) is a private non-profit organisation. Its main goal is to bridge the digital divide in Romania by helping people realise their full potential through the use of technology. The organisation operates projects in two main areas: pre-university education system (training teachers in the use of ICT and working with disadvantaged youth) and the wider community (working with IT and knowledge disadvantaged communities to bring them on board of the information society).[669]

3.18.3. National characteristics

It is difficult to build a detailed picture of the cybersecurity competence in Romania, because the subject is not covered regularly and there have not previously been Romanian think thanks to study the topic. The general perception is that Romanian citizens have not prepared very well for cyber threats because cybersecurity has only started to gain prominence in the media in the last couple years. One reason for this unpreparedness in the cyberspace and the state of digitalisation in general is Romania's previous education system, which did not invest in media literacy or developing digital or cyber skills. For example, it was noted during the Covid-19 pandemic that Romanians easily bought fake news and conspiracy theories.[670]

In 2020, Bucharest was chosen to host ECCC. This new European Cybersecurity Industrial, Technology and Research Competence Centre brings together operators in the public sector and industry and research in this field. The centre manages the EU's cybersecurity research and development funding, worth billions of euros, to be used for encryption and cybersecurity purposes, for example.[671]

3.18.4. The definition of cyber citizen skills

Romania has not clearly defined cyber citizen skills, but they are considered to be closely related to general digital skills concerning navigating the Internet and using applications. Communication emphasises awareness of the consequences of your own actions and social responsibility, because it largely affects the security of others. The aim is to improve education to increase citizens' skills, such as understanding the basic principles of protecting your personal data and equipment. Another goal is to understand the risks and threats posed by digital environment (for example malware, social manipulation, identity thefts) and be aware of the necessary measures (for example use of antivirus software and firewall).[672]

References

[653] GUVERNUL ROMÂNIEI, *Strategia de Securitate Cibernetica a României, pentru perioada 2022–2027* (2022).
[654] GUVERNUL ROMÂNIEI, Strategia de Securitate Cibernetica a României, pentru perioada 2022–2027 (2022).
[655] "National Strategy on the Digital Agenda for Romania 2020," *GUVERNUL ROMÂNIEI,* accessed on January 4, 2023. https://www.gov.ro/en/government/cabinet-meeting/national-strategy-on-the-digital-agenda-for-romania-2020.
[656] "Press release," *Directoratul National De Securitate Cibernetică*, accessed on November 26, 2022. https://dnsc.ro/vezi/document/dnsc-romanian-national-cyber-security-directorate-approved-by-government.
[657] A personal communication to the researcher, 08/06/2022.
[658] "Romania Digilization of Education," *International Trade Administration*, accessed on December 5, 2022. https://www.trade.gov/market-intelligence/romania-digitalization-education.
[659] "Cyber_Education, Cloud_Education and K5-K8 Curricular Reform," *CyberKnowledge Club*, accessed on January 4, 2023. https://cyberknowledgeclub.org/projects/cyber_education-cloud_education-and-k5-k8-curricular-reform/.
[660] "TEORIA CODĂRII ŞI STOCĂRII INFORMAŢIEI," *FSA*, accessed on November 30, 2022. https://www.tcsi.ro/.
[661] "Cyber_Education, Cloud_Education and K5-K8 Curricular Reform," *CyberKnowledge Club*, accessed on January 4, 2023. https://cyberknowledgeclub.org/projects/cyber_education-cloud_education-and-k5-k8-curricular-reform/.
[662] "Information and Computing System Security," *Technical University of Cluj-Napoca*, accessed on November 27, 2022. https://os.cs.utcluj.ro/sisc/.
[663] "Information and Computing System Security," Technical University of Cluj-Napoca, accessed on November 27, 2022. https://os.cs.utcluj.ro/sisc/.
[664] "TEORIA CODĂRII ŞI STOCĂRII INFORMAŢIEI," *FSA*, accessed on November 30, 2022. https://www.tcsi.ro/.
[665] "Romanian Association for Information Security Assurance," accessed on October 24, 2022. https://www.raisa.org/.
[666] "Cyber4kids," accessed on November 26, 2022. https://www.certsign.ro/en/cyber4kids/.
[667] "Mydigiskills," accessed on November 24, 2022. https://mydigiskills.eu/index.php.
[668] "Ora De Net," accessed on October 28, 2022. https://oradenet.ro/public/.
[669] "EOS Romania," accessed on January 4, 2023. www.eos.ro.
[670] A personal communication to the researcher, 19/07/2022.
[671] "Bucharest to host new EU cyber research hub," *Politico*, accessed on November 24, 2022. https://www.politico.eu/article/bucharest-to-host-eus-new-cyber-research-hub/.
[672] "Strategia privind digitalizarea educatiei din Romania 2021-2027," *SMART-Edu*, accessed on December 3, 2022. https://www.smart.edu.ro/#h.xck2kklw9ox5.

3.19. Sweden

ITU, Global Cybersecurity Index (GCI) 2020	26/182 (Global), 15/46 (Europe)
National Cyber Security Index (NCSI) 2022	14/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	4/27

3.19.1. Strategic cyber education and training policies

The national cybersecurity strategy of Sweden, (Nationell strategi för samhällets informations- och cybersäkerhet), introduced in 2017, outlines Sweden's cybersecurity priorities and objectives. Its main goal is to ensure the functioning of parties that are critical to societal functions and the overall security of society. In addition to operators in the public, private and third sector, the strategy intends to improve the know-how of private individuals concerning everyday cybersecurity.[673]

The strategy has six areas or priorities: securing a systematic and comprehensive approach in cybersecurity efforts; enhancing network, product and system security; enhancing capability to prevent, detect and manage cyber attacks and other IT incidents; increasing the possibility of preventing and combating cybercrime; increasing knowledge and promoting expertise; and enhancing international cooperation. It emphasises the responsibility of an ordinary user and highlights the importance of the human factor in the risk management of the cyber world. The first priority concerns concentration and sharing of information to all operators in society, including citizens. The second priority includes secure products, also in consumer markets. The third priority includes services critical to society's functioning that are parts of citizens' everyday lives. The fourth priority addresses cybercrime and also considers consumers. The fifth priority concentrates on increasing the general level of information security competence, which also refers to the competence level of ordinary citizens. The sixth priority concerns international cooperation, but it also has a link to consumers and citizens because it affects international regulation of various services used by consumers, for example.[674]

The Cyber Security Action Plan 2019–2022 was prepared based on the strategy. It specifies the measures and responsibilities concerning each priority. Out of these, especially different campaigns are directly visible to citizens. Campaigns are planned to prevent cybercrime using resources offered by Europol and collaborating with other Nordic countries. The national "Tänk säkert" (Think safe) campaign informs citizens and small companies of cybersecurity threats and data protection. Campaigns are arranged during the European Cybersecurity Month (ECSM), for example.[675]

Sweden wants to be the best country in the world in using the possibilities of digitalisation. This aim is guided by the government's digitalisation strategy, which is the responsibility of the Swedish National Digitalisation Council. The strategy areas are digital competence, security, innovation, infrastructure and management. The goal of digital security is to create optimal conditions for everyone to safely participate and have confidence in the digital society. One of the cornerstones of digital competence is that everyone has sufficient basic digital skills.[676]

3.19.2. The current state of cyber citizen skills education and training

In Sweden, there are several operators in the public, private and third sector who offer training in cyber citizen skills. Authorities responsible for cybersecurity include the Swedish Civil Contingencies Agency (MSB), the Swedish Defence Materiel Administration (FMV), the National Defence Radio Establishment (FRA), the Swedish Armed Forces, the Swedish Post and Telecom Authority (PTS), the Swedish Police Authority and the Swedish

Security Service (Säpo). Together, the authorities have established the National Cyber Security Center for Sweden (NCSC).[677]

The Swedish Civil Contingencies Agency (MSB) offers training for organisations and citizens. Its training course portfolio includes several courses at different levels, from basics of cybersecurity to its own MSB College.[678] The MSB website contains cybersecurity guidance for citizens and reports prepared with authorities to provide more information about cybersecurity[679]. MSB has a free-of-charge e-learning course called Disa ("Digital information security training for everyone") aimed especially at organisations of all sizes. It teaches the basics of cybersecurity and is open for all. The covered topics include secure behaviour, passwords, backups, cloud services, email, social media, checking the sender, malware, cybersecurity outside the workplace and problem situations. Participants receive a certificate for completing the course.[680]

Swedish comprehensive schools teach data processing as part of other subjects. On upper secondary level, you can learn data processing as an optional subject. Security is taught in all grades of comprehensive school as part of learning goals for data processing.[681] According to ENISA's CyberHEAD database, Swedish higher education institutions offer three degree programmes in cybersecurity.[682] The Mastersportal database lists seven degree programmes in cybersecurity or information security offered by University West, KTH Royal Institute of Technology, Stockholm University, Linköping University, University of Skövde, Halmstad University and Luleå University of Technology. According to the websites of the above universities, the programmes are currently available.[683] The Swedish Defence University (Försvarshögskolan) offers training for both security authorities and civilians.[684] In addition, the plan is to establish a Cybercampus specialising in research, training and innovation to strengthen Sweden's cybersecurity.[685]

The Swedish Media Council and Bris, a children's rights organisation, maintain the Swedish Safer Internet Centre (SIC), which belongs to the international Insafe, INHOPE and Better Internet for Kids networks supported by the European Commission. SIC aims to improve cybersecurity of children and adolescents. It works preventively, by providing information and support to children, adolescents, professionals and guardians. For example, SIC produces reports, develops teaching tools and methods and arranges events and campaigns. There are many ways for children and adolescents to participate in the SIC's operation, for example, by joining a youth panel. In addition, the Swedish Media Council coordinates national measures to strengthen the media and information literacy of Swedes.[686] It held the main responsibility for the development of the MIK database and is responsible for its operation. This database contains informative material produced by various operators and aimed at everyone who wants to improve their media and information literacy, from children to seniors. For example, programmes produced by the Swedish Educational Broadcasting Company address topics related to cybersecurity.[687]

The Swedish Internet Foundation is an independent foundation responsible for Swedish domains .se and .nu. It wants to build Internet that has a positive effect on people and society. Its vision is that everyone should want to, dare to and be able to use the internet. The foundation's websites "Internetkunskap" and "Digitala lektioner" have an extensive selection of information and materials for improving digital skills. One area is cybersecurity, and crash courses and articles are available on online scams, passwords, phishing and malware, for example. The websites tell you what to do if you are a victim of an online scam. The Digitala lektioner website also includes ready lessons for different grades of primary and lower secondary school. They comply with the requirements of the curriculum.[688,689]

The Cybersecurity Academy, launched in 2019, aims to provide students in lower and upper secondary education with information about cybersecurity using educational material, lectures and workshops. Young people are offered tools for identifying risks and protecting themselves online. The aim is also to make them curious about technology and information technology. The Cybersecurity Academy offers different educational materials and expert lectures for schools free of charge and continuing education for teachers. Guides to support teaching have also been prepared for teachers in lower and upper secondary school. Free education outside school hours is also available for pupils who are interested in information technology and information security. So far, the

project has reached approximately 340,000 pupils and approximately 4,700 schools. The Cybersecurity Academy has quickly gained popularity. It is a joint project of the Unga Forskare association and IBM supported by MSB, and has numerous partners.[690,691]

Sweden participates annually in the European Cybersecurity Month organised by ENISA. The "Tänk säkert" (Think Safe) campaign mentioned in the Cyber Security Action Plan has been successfully utilised for several years. The aim of the campaign is to develop cybersecurity competence in the entire society by raising awareness on cyber hygiene, such as good password practices, identifying phishing and protecting important information. The campaign website contains information about different topics related to cybersecurity. The materials are aimed at different target groups, such as parents, teachers and over 65-year-olds. Materials have also been published in different languages. You can take a test on the website to see how big of a security risk you are. MSB and the police implement the campaign together, and a large number of partners participate in the distribution of the campaign. During the Cybersecurity Month 2021, the campaign reached 12.6 million citizens (1.5 million in 2020). More than 60 webinars and lectures were arranged during the month. A study conducted in connection with the campaign showed that people's cybersecurity behaviour changes slowly, calling for long-term campaign work. The achieved results have demonstrated the importance of the campaign.[692,693,694]

3.19.3. National characteristics

Sweden is one of the most digital countries in the world. That brings numerous benefits but also risks – Sweden is an attractive target for cyber attacks, making it vulnerable. Generally, the cybersecurity competence of Swedes is still not sufficient, even though the situation has improved during recent years. According to the Swedish Internet Foundation, general Internet skills should be improved to ensure that more people understand the risks of digital services and know how to prevent them. For example, it has been suggested that cybersecurity could be taught as a separate subject in primary and lower secondary school.[695,696]

A report on the Internet behaviour of Swedes (2022) says that the majority of citizens restrict their Internet use in some ways. The most common reasons for this are protecting your privacy and worrying about online scams. Younger users are more concerned about their privacy. Seniors on the other hand are more afraid of hackers and fraudsters. Half of Swedes restrict their Internet use in some way due to insecurity.[697]

3.19.4. The definition of cyber citizen skills

According to the Swedish National Digitalisation Council's definition, digital competence entails: 1) the ability to seek information, communicate, interact and produce content digitally, 2) the capacity to use digital tools and services, 3) the understanding of the change in society brought by digitalisation, along with its opportunities and risks, and 4) the motivation to participate in the development effort. Digital competence is visible in four areas of life: private life, social life, education and working life.[698] Cyber citizen skills have also been defined based on the DigiComp framework. DigComp 2.2 version was published in Swedish in October 2022.[699] The "Tänk säkert" (Think safe) campaign describes how every citizen can contribute to cybersecurity in Sweden. Instructions are given about good password practices, secure e-identification, backups and protecting against malware, ransomware and phishing.[700]

References

[673] Government Offices of Sweden, *Ministry of Justice, A national cyber security strategy, Skr. 2016/17:213* (2017).
[674] Government Offices of Sweden, *Ministry of Justice, A national cyber security strategy, Skr. 2016/17:213* (2017).
[675] Swedish Civil Contingencies Agency (MSB), *Comprehensive Information and Cyber Security Action Plan for the years 2019–2022* (2020).
[676] "Sveriges digitalisering," *Digitaliseringsrådet*, accessed on December 14, 2022. https://digitaliseringsradet.se/sveriges-digitalisering/.
[677] "Vårt uppdrag: Att stärka Sveriges samlade förmåga att förebygga, upptäcka och hantera cyberhot," *Nationellt cybersäkerhetscenter*, accessed on 14 December 2022, https://www.ncsc.se/.
[678] "Training and exercises," *Swedish Civil Contingencies Agency (MSB)*, accessed on December 13, 2022. https://www.msb.se/en/training--exercises/.
[679] "Informationssäkerhet," *MSB Myndigheten för Samhällsskydd och Beredskap*, accessed on December 13, 2022. https://www.msb.se/sv/rad-till-privatpersoner/informationssakerhet/.
[680] "Digital informationssäkerhetsutbildning för alla (Disa)," *MSB Myndigheten för Samhällsskydd och Beredskap*, accessed on December 16, 2022. https://www.msb.se/sv/utbildning--ovning/alla-utbildningar/datorstodd-informationssakerhetsutbildning-for-anvandare-disa/.
[681]European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 23-53.
[682] "CYBERHEAD - Cybersecurity Higher Education Database," *ENISA*, accessed on December 13, 2022. https://www.enisa.europa.eu/topics/cybersecurity-education/cyberhead#/.
[683] "Studyportals," accessed on December 14, 2022. https://www.mastersportal.com/study-options/268861763/cyber-security-sweden.html.
[684] "Swedish Defence University," accessed on December 13, 2022. https://www.fhs.se/en/swedish-defence-university.html.
[685] "Cybercampus Sweden," accessed on December 14, 2022. https://cybercampus.se/.
[686] "Swedish Safer Internet Centre," *Better Internet for Kids*, accessed on 13 December 2022, https://www.betterinternetforkids.eu/sic/sweden.
[687] "MIK Sveriges kunskapsbank," *Statens Medieråd*, accessed on December 13, 2022. https://www.statensmedierad.se/mik-sveriges-kunskapsbank.
[688] "Säkerhet på nätet," *Internetkunskap, Internetstiftelsen*, accessed on December 15, 2022. https://internetkunskap.se/sakerhet-pa-natet/.
[689] "Fria lektioner i digital kompetens," *Digitala Lektioner, Internetstiftelsen*, accessed on December 15, 2022. https://digitalalektioner.se/.
[690] "Cybersecurity Academy," *Unga Forskare*, accessed on December 16, 2022. https://ungaforskare.se/cybersecurityacademy/.
[691] "Stärk ungas kunskaper inom cybersäkerhet," *Cybersecurity Academy*, accessed on December 16, 2022. https://cybersecurityacademy.se/.
[692] "Informationssäkerhetsmånaden," *MSB Myndigheten för Samhällsskydd och Beredskap*, accessed on December 14, 2022. https://www.msb.se/sv/amnesomraden/informationssakerhet-cybersakerhet-och-sakra-kommunikationer/informationssakerhetsmanaden/.
[693] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 139-140.
[694] ENISA, *Cybersecurity Education Initiatives in the EU Member States* (2022).
[695] Emmy Englund and Linnéa Tullin, *Cybersäkerhet, En kartläggning av Sveriges nuläge 2020 och framtidsutsikter för branschen* (2020), 20–21.
[696] Digitaliseringsrådet, *En lägesbild av digital trygghet* (2018), 22.
[697] "Svenskarna och internet 2022," *Internetstiftelsen*, accessed on December 15, 2022. https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2022/.
[698] Digitaliseringskommissionen, *Gör Sverige i framtiden – digital kompetens* (SOU 2015:28), 102–103.
[699] "Lansering av DigComp 2.2 på svenska," *Dataföreningen*, accessed on December 15, 2022. https://dfs.se/pa_gang/lansering-av-digcomp-2-2-pa-svenska/.
[700] MSB Myndigheten för Samhällsskydd och Beredskap, *Alla kan bidra till Sveriges cybersäkerhet. Du också! Tänk säkert*, https://rib.msb.se/filer/pdf/30140.pdf.

3.20. Germany

ITU, Global Cybersecurity Index (GCI) 2020	13/182 (Global), 5/46 (Europe)
National Cyber Security Index (NCSI) 2022	6/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	13/27

3.20.1. Strategic cyber education and training policies

In recent years, Germany has adopted several strategies related to cybersecurity, such as the National Plan for Information Infrastructure Protection in 2005, the first Cyber Security Strategy in 2011, the second Cyber Security Strategy in 2016 and the latest update of the Cyber Security Strategy for Germany in 2021.[701] In Germany, the Federal Ministry of the Interior and Community (Bundesministerium des Inneren, BMI) plays an important role in matters related to national and cybersecurity. BMI works in close cooperation with the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, BSI) and aims to develop information and cybersecurity of the federation. In 2011, BMI published the Cyber Security Strategy for Germany (Cyber-Sicherheitsstrategie für Deutschland 2011). In this strategy, the Government emphasised the importance of cyber strategy as part of Germany's altered security environment. The Cyber Security Strategy for Germany was updated in 2016 and 2021. From the beginning, Germany has adopted a technical and preventive approach to cybersecurity with a focus on protecting information systems and critical infrastructure from the perspective of civil defence.[702] The Cyber Security Strategy updated in 2016 has been characterised as the first strategy to focus on special needs of individual users in addition to social aspects.[703] The whole-of-society approach set out in the strategy of 2016 also initiated the implementation of a national cybersecurity agreement. The objective of the agreement is to strengthen the shared responsibility of all actors in society for digital security.[704] According to the strategy of 2016, responsible behaviour in cyberspace and opportunities brought by the Internet as well as the related risks are an essential part of today's civic digital skills. Because of this, digital education must be integrated into the country's educational system. The aim of the Federation is to ensure that when young people finish school, they have sufficient knowledge and competence concerning the security of information technology. According to the strategy, the Government wants to increase and extend the course portfolio in the IT sector by increasing the number of study places in universities and supporting the leading institutions particularly in the field of computer science, including big data analyses, industrial software and IT security.[705]

3.20.2. The current state of cyber citizen skills education and training

In line with the Cyber Security Strategy for Germany, cybersecurity education has been added to all educational levels, and several universities offer study modules and Master's programmes in cybersecurity. According to ENISA (the European Union Agency for Cybersecurity), there were five higher education programmes focused on cybersecurity in Germany in 2022.[706] In addition to education programmes, nearly every German university offers IT studies, which also include study modules in information security and cybersecurity.

BSI has an important role in developing and maintaining cybersecurity in Germany. BSI offers extensive information about information security and cybersecurity in active cooperation with various organisations and the private sector. It provides citizens with information on how to protect against different cyber attacks and what to do if you become a victim of a cyber attack. Material is also available in the form of educational videos. BSI has also implemented several campaigns to improve citizens' cybersecurity competence.

In Germany, training and education related to cybersecurity have been integrated into the educational system. As a result, it includes mainly studies for pupils and students in education institutions, like the Cyber Security Strategy 2016 points out. The need to offer citizens basic training on cybersecurity has been acknowledged in Germany but at the moment, training is mostly arranged by different associations and the private sector. The Deutschland sicher im Netz e.V. (DsiN) association was established in 2006 for the above purpose at the first national IT Summit. Supported by BMI, DsiN aims to support consumers and smaller companies to operate securely and confidently in the digital world. Together with its members and partners, DsiN offers help and information about secure Internet use for private individuals of all ages, both at work and in their everyday life. Support is available as different educational materials and check lists. In addition to private individuals, DsiN also offers support for small and medium-sized companies.[707]

In addition to BSI and DsiN, the German Safer Internet Centre plays an important role in offering information security and cybersecurity training for citizens and particularly children. The centre has been running since 2008, and it has combined services focused on secure Internet use and guidance into one when they were previously funded separately. Such services include the Klicksafe service, Internet support lines internet-beschwerdestelle.de and jugendschutz.net, as well as Nummer gegen Kummerin, a helpline for children, adolescents and their parents. The German Safer Internet Centre is part of the strategy developed by the European Commission in 1999 to increase citizens' awareness on secure Internet use. The programme finances centres that specialise in secure Internet use (Safer Internet Centres) in 27 European countries, including Germany. The main objective of these centres is to raise the awareness of children, parents, teachers and youth workers on the risks related to Internet use and offer young people advice on secure Internet use. Safer Internet Centres also include hotlines to receive reports from the public about illegal content online.[708] As part of the German Safer Internet Centre, a youth panel was established in 2009 at an academic secondary school in Rhineland-Palatinate. It offers young people a place where they can express their views and opinions and exchange knowledge and experiences on the use of different network technologies. In addition, the German Awareness Centre, hotlines and helpline work together with relevant organisations on the national and European level, and participate in awareness raising events and campaigns, such as the Safer Internet Day.[709]

Klicksafe is a joint project of two German Media Authorities: the Central Authority for Media and Communication of Rhineland-Palatinate (LMK), responsible for coordination, and the Media Authority of North Rhine-Westphalia (LfM). The statutory obligations of Media Authorities include licensing, providing support, promoting media literacy and overseeing telemedia. The overseeing task is managed by the Commission for the Protection of Minors in the Media (KJM). KJM is a full member of LMK.[710] Klicksafe aims to promote people's online competence. The service is intended for people who support children and young people in developing their Internet skills, and it offers an overview of current online topics and concrete tips and lessons for everyday digital life. The service's information portal provides users with up-to-date information, practical tips and helpful materials on digital services and related topics. Klicksafe also arranges related campaigns. In addition, it implements training courses for children, young people, parents, teachers and professionals on Internet use and risks of the Internet. Klicksafe's objective is to promote media literacy on the Internet. Klicksafe works actively in Germany and elsewhere in Europe and publishes information packages and relevant publications for different target groups. The Klicksafe website also contains interactive exercises where users can practice their IT skills, in game-like fashion and otherwise.[711]

IMC is a private sector company established by the German Saarland University. It offers holistic support for the public sector, companies and educational institutions in designing and implementing digital educational strategies. IMC also offers e-learning environments and different games. One of these games is Cyber Crime Time, offered to private individuals under a free licence and to companies under a paid licence. The idea of the game is based on topics related to cybercrime, and it coaches the users to identify and prevent various cyber risks. The topics are related to, for example, social manipulation of users, creating secure passwords, phishing, threats associated with remote working, various malware and ransomware, identity thefts and security threats in public wireless networks.[712]

3.20.3. National characteristics

In Germany, cybersecurity is considered a crucial part of home and foreign affairs as well as security policy. Over the years, an extensive and dense network of actors with numerous interconnections at the national and international level has emerged in Germany. The network creates a foundation for a structured and sustainable cybersecurity policy. This rather complicated ecosystem is described in a publication called "Germany's Cybersecurity Architecture", published biannually by Stiftung Neue Verantwortungin (SNV), an expert organisation.[713] The very comprehensive Wirtschaftsinformatik Conference is arranged annually in Germany. The addressed topics are digitalisation and cybersecurity from the perspective of social functions.[714] The separate Dagstuhl Institute arranges short dialogues, discussions and exchanges of ideas with stakeholders in the science community around the year, for example, on cybersecurity.[715]

The German states enjoy a high degree of autonomy, and this is also reflected in cybersecurity issues. Some states, like Nordrhein-Westfalen, have prepared their own cybersecurity strategy based on the goals defined in the national cybersecurity strategy. The strategy emphasises, for example, the importance of the information security and cybersecurity competence of private individuals in terms of holistic cybersecurity.[716] The Federal Ministry of Research and Technology coordinates collaboration between the Federation and the states as well as international and EU collaboration in educational matters, and the education policy is mainly the responsibility of the states. That is why the organisation of the educational system and decision-making does not take place at the Federal level but has been assigned to the Ministries of Education in each 16 states. As a result, regulation concerning the offered degree programmes and curricula varies state by state, which is also reflected in the offered cybersecurity training. Differences between the states are also affected by differences in the quality of the digital infrastructure and the strict data protection policy, restricting the utilisation of remote learning and digital learning environments, for example. After the amendment of the constitution in 2019, the German federation has been able to support the states financially in the educational sector and promote cooperation between the states, especially in issues related to the development of digitalisation.[717]

3.20.4. The definition of cyber citizen skills

Cyber citizen skills include basic skills required in cyberspace which citizens need in their everyday lives to improve their security and the security of others. #einfachaBSIchern, an information campaign implemented by the Federal Ministry of the Interior and Community (BMI) and the Federal Office for Information Security (BSI), focuses on improving the citizens' knowledge and skills related to digital security. The campaign aims to develop citizens' cyber skills, such as awareness of the threats in the cyber world, understanding of the value of digital information for different parties and the importance of having the basic skills to protect data.[718]

References

[701] Martin Schallbruch and Isabel Skierka, "The Evolution of German Cybersecurity Strategy," *Cybersecurity in Germany* (Springer Cham, 2018), 15, doi: 10.1007/978-3-319-90014-8.
[702] Schallbruch and Skierka, "The Evolution of German Cybersecurity Strategy," 16.
[703] Schallbruch and Skierka, "Cybersecurity in Germany," 27.
[704] Bundesministerium des Innern und für Heimat, *Online kompendium Cybersicherheit in Deutschland: National Pakt Cyber Sicherheit* (Bundesministerium des Innern, für Bau und Heimat, 2021), 1.
[705] Federal Ministry of the Interior and Community, *Cyber Security Strategy for Germany*, (Federal Ministry of the Interior, Building and Community, 2016), 10.
[706] "CYBERHEAD - Cybersecurity Higher Education Database", *ENISA*, accessed on November 30, 2022. https://www.enisa.europa.eu/topics/education/cyberhead#/.
[707] "DsiN," Deutschland sicher im Netz, accessed on 25 October 2022, https://www.sicher-im-netz.de/.
[708] LMK, LfM, eco, FSM, jugendschutz.net and NgK, *Final public report for publishing, SI-2009-SIC-123906, Safer Internet DE SIC* (Safer Internet plus, 2012).
[709] LMK etc., *SI-2009-SIC-123906.*
[710] "Klicksafe," *Media Authority Rhineland-Palatinate,* accessed on September 12, 2022. https://www.klicksafe.de.
[711] "Klicksafe".
[712] "Part of scheer," *imc*, accessed on October 11, 2022. https://www.im-c.com.
[713] "Deutschlands staatliche Cybersicherheitsarchitektur," *Stiftung Neue Verantwortung*, accessed November 10, 2022. https://www.stiftung-nv.de/de/publikation/deutschlands-staatliche-cybersicherheitsarchitektur.
[714]"W23," *Universität Paderborn*, accessed on 27 December 2022, https://wi2023.de/en/scientific-tracks/
[715] "Schloss Dagstuhl Where Computer Scientists Meet," *Leibniz-Zentrum für Informatik GmbH*, accessed on December 27, 2022. https://www.dagstuhl.de/en/
[716] Hendrik Wüst and Herbert Reul, *Cybersicherheitsstrategie des Landes Nordrhein-Westfalen* (Die Landesregierung Nordrhein-Westfalen, 2021).
[717] "Saksan koulutusjärjestelmä, koulutusalan toimijat ja suurtapahtumat koulutusviennin näkökulmasta", *Embassy of Finland, Berlin*, accessed on November 13, 2022. https://finlandabroad.fi/web/deu/ajankohtaista/-/asset_publisher/TV8iYvdcF3tq/content/saksan-koulutusjarjestelma-koulutusalan-toimijat-ja-suurtapahtumat-koulutusviennin-nakokulmasta/384951.
[718] "#einfachaBSIchern," Bundesamt für Sicherheit in der Informationstechnik, accessed on November 13, 2021. https://www.bsi.bund.de/DE/Themen/Kampagne-einfach-absichern/kampagne_node.html.

3.21. Slovakia

ITU, Global Security Index (GCI) 2020	34/182 (Global), 21/46 (Europe)
National Cyber Security Index (NCSI) 2022	17/160 (24 October 2022)
The Digital Economy and Society Index (DESI, 2022)	23/27

3.21.1. Strategic cyber education and training policies

Slovakia's National Cybersecurity Strategy 2021–2025 was published in 2021. It has a simple aim: to prepare and bring Slovakia to the level at which it is always one step ahead of a potential threat. The vision of the National Security Authority is to strengthen and create an open, free and secure cyberspace for everybody. In cyberspace, fundamental human rights and freedoms are of utmost importance. The Slovak Republic promises to respect fundamental human rights and promote the status of human rights both offline and online. The Slovak Republic supports and enforces the status of human rights in the long term and commits to other states with the same value system. It also supports the responsible behaviour of other countries and a uniform interpretation of international law in cyberspace.[719] The Cybersecurity Strategy emphasises continuous capacity building in the field of cybersecurity. It defines a concept that combines the efforts of the state to ensure a high level of cybersecurity with the responsibility of individuals for carrying out activities aimed at their own security. The main goal is to ensure that professionals and citizens have a sufficient level of competence in cybersecurity. According to the action plan, the Ministry of Education, Science, Research and Sport of the Slovak Republic (Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky) is responsible for innovative educational systems in the field of cybersecurity at primary and lower secondary schools and upper secondary schools, and special education and specialists in the upper secondary level and higher education. A new professional education system is planned to train more professionals and to raise security and situational awareness of threats, vulnerabilities, incidents and protection methods in the cyberspace.[720]

According to the strategy, education is one of the main areas of cybersecurity, allowing development and improvement of cybersecurity capabilities. Building the security awareness of ordinary users, acts as a precaution against cybersecurity incidents, because educated users can better respond to security threats. At the moment, cybersecurity education is not systematic, and only one university programme is offered in the field of cybersecurity. This is due to the lack of cybersecurity teachers. Several private special courses and training programmes are offered but they cannot replace systematic public education. There is no security awareness building and basic security education in the area of responsible behaviour on the Internet from primary schools up to secondary schools, despite the fact that a considerable number of users are achieving this level. The education of public administration staff has not been systematic. The risks of cyberspace and prevention of cyber attacks are not addressed in primary and secondary school and as a consequence, people may not really be aware of cyber threats. It is important to understand what it means to include security awareness in the education system. An educated person not only understand the problem but can also proactively identify it.[721]

In 2019, the Ministry of Investments, Regional Development and Informatization of the Slovak Republic (Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky) published the Digital Transformation Strategy for Slovakia (Stratégia digitálnej transformácie Slovenska 2030).[722,723] The strategy aims to provide more efficient support for education in the digital era. The courses teach students and teachers to understand the importance of their own conscious activities, creating and maintaining a secure digital identity for individuals and companies, analysing and classification of data and basic skills required for a deeper understanding. Teaching of information technology, such as software coding, is started at an early age. The aim

is to prepare education for systematic classification of data and continue activities until 2030. The classification of data emphasises competence in the digital era and the digital transformation of education in schools. The aim is also to support development of digital skills and competence from early age to ensure that everyone has the necessary skills in the digital world. At the same time, the use of digital technologies is supported to promote successful education. Systems are built to support life-long learning of digital skills. An analysis of the state of digital skills in Slovakia and effective mechanisms to prevent disinformation are being planned. The objective is to make Slovakia a modern country by 2030 where innovative and ecological industry benefits from digital data economy. Slovakia wants to become an information society where citizens can fully realise their potential and live secure quality life in the digital era. The strategy is targeted to ordinary citizens who should have an easier and higher quality everyday life at the workplace as well as in the private life, and citizen-entrepreneurs who should benefit from reduced paperwork burden to the maximum possible extent and be supported by adequate incentives.[724]

3.21.2. The current state of cyber citizen skills education and training

The National Cyber Security Centre (Národné centrum kybernetickej bezpečnosti, SK-CERT) is part of the national security authority. It aids governance, development, management and support of cybersecurity competence centres, including training, educational activities, and research.[725] These centres of excellence, research and cybersecurity competence include: European Union Agency for Cybersecurity (ENISA), Cyber Security & Infrastructure Security Agency of the United States (US-CERT), CERT.org, Carnegie Mellon University in the United States and the National Cyber Security Centre's TURLA group).[726,727,728,729]

The only university offering a Master's programme in the field of cybersecurity is the Slovak University of Technology in Bratislava, which offers Information Security as a Master's programme.[730]

The Slovakian Safer Internet Centre (SK SIC) has three components: the awareness centre Zodpovedne.sk, Helpline and Stopline.[731] SK SIC's philosophy is reflected in the graphic communication. The symbol of the centre resembles a child's hand and the acronym www, and the colours are the same as traffic lights. Green light is shown for responsible use of internet and modern technologies. Orange means a helping hand. Red symbolises a STOP sign for illegal content and activities on the Internet. The aim of the awareness centre is to educate parents and teachers on safer Internet use and to introduce special tool kits to improve awareness and services together with third parties (schools).[732,733,734,735,736]

SK SIC designs awareness campaigns and resources for children, parents, grandparents, teachers and social workers. The objective is to provide children with the digital skills and tools they need to safely navigate the Internet. It promotes parents' and children's awareness of high-quality online content and makes the associated resources available through its services. It evaluates the impact of the awareness campaigns on the target groups and provides qualitative and quantitative feedback at European level. SK SIC establishes and maintains partnerships and promotes dialogue and exchange of information with key players (government agencies, ISPs, user organisations, education stakeholders) at national level.[737]

SK SIC has operated since 2007, continuously implementing the goals of the Safer Internet programme and the Safer internet Plus programme During the last eight years, SK SIC has established its position in the protection of children and adolescents on the Internet. It contributes to the development of best practices in Europe and around the world. SK SIC maintains eight websites and five social media channels, with 14.1 million views and almost seven million downloads of online tools so far. There are more than 11,000 media publications. SK SIC has trained more than 50,000 adults (including teachers, parents and social workers), 123,000 children and adolescents, and reached more than one million children and adolescents. The Hotline has received more than 11,000 reports. SK SIC is also actively involved in the legislation process concerning Internet security. It has received over 20 awards, demonstrating the excellence of its activities and tools.[738]

CyberGame[739] is a cybersecurity game intended for students, talented gamers and professionals of different levels. It is a biannual tournament. The next tournaments will be organised in March and May 2023. CyberGame includes tasks at various difficulty levels, and players can earn prizes in different categories. The game includes four main branches, each with different scenarios and a total of 50 tasks. These include malware analysis where the players must find out how malicious code works, scenario application and cryptography where you analyse how encrypted and coded files work. One section is a forensic analysis where the player must look for digital hints from data collected from infected computers, and a scenario which includes Open Source Intelligence (OSINT) analysis[740] where players learn about malicious activity or malware based on open source and Internet searches. SK-CERT, Slovakia's National Cyber Security Centre recommends the game.

Guardians is an online competition for companies. It is a game where companies can test their competence against others. Tested skills include digital skills online, investigation of cyber events and looking for vulnerabilities. Despite the sharp increase in the number of cyber attacks, cybersecurity is still underrated and underfinanced in several companies. The aim of the Guardians game is to raise general awareness on of cybercrime and its negative impact on all aspects of society. The next event will be arranged in 2023.[741]

3.21.3. National characteristics

Unlike other European countries, Slovakia considers fundamental human rights and freedoms one of the key points of its cybersecurity strategy.[742] Cyberspace must be considered as an environment, similar to the physical world. To make it safe, we must apply clear rules to cyberspace which respect fundamental human rights and guarantee the rights and freedoms guaranteed by the constitution, including the right to privacy online. Information and awareness must be open for all, free and accessible everywhere. The security of cyberspace must be linked to its freedom. Fundamental human rights and freedoms in the digital world can be guaranteed only if digital sovereignty is upheld in EU countries. It also ensures independence and sovereignty in cyberspace.[743]

3.21.4. The definition of cyber citizen skills

Slovakia has not specifically defined cyber citizen skills. Digital skills and cybersecurity skills are determined by the national framework provided in Slovakia's national cybersecurity strategy. The concept of "safe Internet for all" is created and awareness is continuously raised in the field of cybercrime with a focus on a wide range of population and the most vulnerable groups, such as children and seniors. Life-long learning of digital skills is also highlighted in terms of raising citizens' awareness and preparing for cybersecurity threats. Emphasis is on the responsibility of citizens in the digital world and online. It affects everyone's cybersecurity, both on national level and in users' inner circle.[744] The Digital Transformation Strategy for Slovakia can be seen as a contribution to the definition of cyber citizen skills.[745]

References

[719] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021–2025* (2021).
[720] "Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky," accessed on October 28, 2022. https://www.minedu.sk/.
[721] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021–2025* (2021).
[722] "Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky," accessed on December 3, 2022. https://www.mirri.gov.sk/index.html.
[723] "Stratégia digitálnej transformácie Slovenska 2030," accessed on December 3, 2022. https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/.
[724] "Stratégia digitálnej transformácie Slovenska 2030," accessed on November 29, 2022. https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/index.html.
[725] "Národné centrum kybernetickej bezpečnosti SK-CERT," accessed on November 26, 2022. https://www.sk-cert.sk/sk/o-nas/index.html.
[726] "European Union Agency for Cyber Security," accessed on December 6, 2022. https://www.enisa.europa.eu/.
[727] "US-Cert, Cyber Security & Infrastructure Security Agency," accessed on December 6, 2022. https://www.cisa.gov/uscert/.
[728] "Cert.org, Carnegie Mellon University," accessed on 6 December 2022, https://www.cmu.edu/.
[729] "Turla Group Malware," *National Cyber Security Centre*, accessed on December 6, 2022. https://www.ncsc.gov.uk/news/turla-group-malware.
[730] "Information Security," *Slovak University of Technology*, accessed on December 1, 2022. https://www.fiit.stuba.sk/study-programs.html?page_id=2090.
[731] "Stopline.sk," accessed on November 24, 2022. https://stopline.sk/sk/uvod/.
[732] "Stopline.sk," accessed on November 24, 2022. https://stopline.sk/sk/uvod/.
[733] "Zodpovedne.sk," accessed on November 26, 2022. https://www.zodpovedne.sk/index.php/sk/.
[734] "Pomoc.Sk Helpline," accessed on November 24, 2022. https://pomoc.sk/.
[735] "Stopline.sk," accessed on November 24, 2022. https://stopline.sk/sk/uvod/.
[736] "Slovak Safer Internet Centre," accessed on November 22, 2022. https://www.zodpovedne.sk/index.php/en/.
[737] "Slovak Safer Internet Centre," accessed on November 22, 2022. https://www.zodpovedne.sk/index.php/en/.
[738] "Slovak Safer Internet Centre," accessed on November 22, 2022. https://www.zodpovedne.sk/index.php/en/.
[739] "Cybergame," accessed on November 22, 2022. https://cybergame.sk-cert.sk/.
[740] "OSINT Analytics," accessed December 4, 2022. https://www.osintanalytics.com/.
[741] "Guardians," accessed on November 26, 2022. https://www.guardians.sk/.
[742]Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021-2025, accessed on November 22, 2022. https://www.nbu.gov.sk/wp-content/uploads/cyber-security/National_cybersecurity_strategy_2021.pdf.
[743] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021–2025* (2021).
[744] National Security Authority, *Slovenskú národnú stratégiu kybernetickej bezpečnosti 2021–2025* (2021).
[745] "Stratégia digitálnej transformácie Slovenska 2030," accessed on 02/12/2022, https://www.mirri.gov.sk/sekcie/informatizacia/digitalna-transformacia/strategia-digitalnej-transformacie-slovenska-2030/.

3.22. Slovenia

ITU, Global Cybersecurity Index (GCI) 2020	67/182 (Global), 34/46 (Europe)
National Cyber Security Index (NCSI) 2022	51/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	11/27

3.22.1. Strategic cyber education and training policies

In Slovenia, Digital Slovenia 2020 is an umbrella strategy, and the Cyber Security Strategy 2016 is an associated document. The comprehensive goals of digitalisation include making Slovenia an inclusive digital society and creating security and confidence in cyberspace by raising citizens' cyber awareness, improving digital literacy and protecting privacy and cultural identity.[746] Digital Slovenia 2030 strategy and a new national cybersecurity strategy are under preparation.[747]

Slovenia's Cyber Security Strategy 2016 puts a strong emphasis on the importance of awareness for cybersecurity. Increasing awareness and education help eliminate risks and create a culture of secure use of technology. Slovenia is building awareness raising programmes, and the methods and content are adapted to each target group as optimally as possible. With regard to children and adolescents, topics related to cybersecurity will be included in the curriculum at different levels of education. Adjusted programmes are created for the other members of the population and companies [748] In Slovenia, the academic research community contributes to ensuring cybersecurity by increasing awareness, education and research through its education programmes and related courses on all levels of education and through the results of research organisations. Slovenia's cybersecurity model is open to civil society's initiatives. Particular attention is paid to initiatives for improvements and assistance in raising awareness by professional associations. Raising awareness is considered important because it improves the cybersecurity culture and teaches users to independently take care of their own security in cyberspace. Therefore, in addition to further implementation of the existing awareness raising programmes, new ones will be developed, participation in projects is encouraged and the civil society is involved in these activities. Effective outreach is focused on specific target groups (for example children, citizens of different ages and business entities). Measures to ensure citizens' cybersecurity are regular implementation of awareness raising programmes and introducing cybersecurity content in education programmes. The aim is to include topics related to cybersecurity in the curricula of schools at all levels of the education system. Universities are encouraged to offer independent study programmes on cybersecurity. In addition, the competence of the cybersecurity staff of key stakeholders is ensured by continuous training and certification.[749]

3.22.2. The current state of cyber citizen skills education and training

Slovenia has two publicly financed projects to raise cybersecurity awareness: 1) SI-CERT's "Safe on the Internet" programme[750] and 2) the "Safer Internet Centre Slovenia" programme (SIC) and the SAFE.SI awareness centre operated under the SIC programme.[751] The first project, "Safe on the Internet", is aimed at the general public, but it also contains special content for SMEs (small companies, artisans and entrepreneurs). This project also participates in the campaigns of the EU's Cybersecurity Month. The second project, Safer Internet Centre, is aimed at children and adolescents as well as their parents and other educators (for example teachers and youth workers). It is run by a consortium of partners coordinated by the Faculty of Social Sciences at the University of Ljubljana. The Office of the Republic of Slovenia for Information Security (URSIV) partly or fully finances both information programmes.[752,753,754] SI-CERT also participates in the SAFE.SI project.[755]

The “Safe on the Internet” project financed by URSIV is intended to be a long-term project. Its main objective is to help improve the information security literacy of ordinary internet users. The project also has short-term objectives. The programme wants to raise awareness on different cyber threats, give advice on the use of online banks, provide instructions for secure online shopping and selling as well as inform people of various online frauds. The website provides users with information, guidance and practical solutions for protecting yourself and your identity in social networks. The project’s target group is the general public, and emphasis is on adult users (approximately 24–54-year-olds) because they are the main users of online shops, online banks and social media. Another target group is SMEs because they have limited budgets for professional IT support. CI-CERT has produced numerous materials during the last decade. The most important communication channel is the Varninainternetu.si learning portal. The website contains more than 500 articles, the latest news and notifications of information security threats. Social media channels (for example Facebook, Instagram) are also an important part of the activities and communication, as well as the Safe News newsletter and various physical materials, such as brochures, posters and educational videos (40 videos on cybersecurity). At the end of last year, a cybersecurity course called “Varni v pisarni” (Safe at the office) was launched for SMEs.[756] Another programme, awareness centre SAFE.SI operating under the “Safer Internet Centre Slovenia” (SIC) programme, is initiated and partly funded by the EU. The project is financed by the Office of the Republic of Slovenia for Information Security (URSIV) and the European Health and Digital Executive Agency (HaDeA). The project is responsible for raising awareness in the target group (children and adolescents, parents and professional educators).[757] School population is included in the programme (both online and in classroom) as well as children in kindergartens, at least partially.[758] SIC belongs to the EU’s Better Internet for Kids programme. In addition to the awareness centre and the Safe.si website, with own sections for both target groups, the SIC programme includes “TOM-telefon”, a helpline for adolescents and their parents which provides help in difficult situations, and hotline “Spletno oko”.[759,760]

There is an active effort to attract young people’s interest in cybersecurity. In 2021, URSIV launched the Cyber Talent project to increase cybersecurity’s popularity. The project arranges online cybersecurity workshops and finances the training of the Slovenian team and its participation in the annual European Cybersecurity Challenge. In this context, URSIV is also planning cooperation with secondary education institutions, faculties and companies to create an ecosystem to develop cybersecurity capabilities.[761] IT or cybersecurity is included in the studies of several higher education institutions, such as the curricula of the University of Maribor, the University of Ljubljana and the private GEA College.[762] In Slovenia, training in cybersecurity and civic digital skills is available as e-learning programmes for primary and lower secondary schools and teachers. You can also get a Bachelor's degree through e-learning programmes. Vocational education and certification systems are also available for companies and educational institutions.[763] Lifelong learning is invested in. For example, the Ministry of Labour, Family, Social Affairs and Equal Opportunities (MoLFSA) and the Public Scholarship, Development, Disability and Maintenance Fund of the Republic of Slovenia have established measures to upskill employees, especially the active ageing workforce. These programmes develop digital skills, such as the use of digital tools and software and digital communication. The Administration Academy arranges digital skills courses for civil servants.[764]

The Slovenian Safer Internet Centre (SIC) uses posters, pamphlets and e-books to provide tips and tools for safe internet use. For example, “Vzgoja za internet”, a 44-page user manual, tells parents how to teach internet use for children. Slovenia places a strong emphasis on citizens’ welfare in cyberspace. It focuses on digital wellbeing topics. The programme includes, for example, instructions for using the wellbeing settings of phones and tablets for over 25-year-olds and a quiz in digital wellbeing for 10–12-year-olds and 12–15-year-olds. Many of these campaigns have been produced by the Faculty of Social Sciences at the University of Ljubljana.[765] SIC also has a few mobile applications.[766,767] “Odklikni” (Click) addresses cyber violence and “Reši spletno dilemo!” (Solve an online dilemma) helps you to make decisions online.

URSIV intends to prepare and introduce cybersecurity themes in the curricula of primary and lower secondary education. In this context, URSIV cooperates with the Government Office for Digital Transformation (Služba vlade za digitalno preobrazbo), which plans to include mandatory ICT programmes in the school curricula, and

with the Ministry of Education, Science and Sport of the Republic of Slovenia (Ministrstvo za izobraževanje, znanost in šport). So far, this has been funded under Slovenia's Recovery and Resilience Plan, and materials are prepared in cooperation with certain faculties.[768]

Two target groups, seniors and people with disabilities, have not been sufficiently considered in cybersecurity campaigns and education. For people with disabilities, the solution would be to make the existing materials user-friendly. User-friendliness is required for new materials. Seniors do not commonly have advanced technological skills, and programmes for them will probably be connected to programmes for improving digital literacy.[769] In the future, the aim is to produce more different programmes for different skills and educational levels and for awareness raising programmes. New Master's and Doctoral programmes are currently being introduced.[770] In the future, Slovenia wants to improve citizens' awareness of cybersecurity and increase information about possible cyber threats and identifying basic cyber risks for ordinary citizens.[771] Up-to-date and constantly updated education programmes are also required because cyber threats are constantly evolving.[772]

Slovenia won the best video for European Cybersecurity Month 2022 with its video "Darko wants to take his girlfriend on a trip", which addresses online scams.[773] The winning material will be subtitled in all official EU languages. The reference contains a link for a version with subtitles in English.[774]

3.22.3. National characteristics

Slovenia's Cyber Security Strategy emphasises fairness and the importance of individual cybersecurity. Everyone must be able use ICT as safely as possible, while respecting privacy and human rights. Citizens must have the opportunity to become acquainted with the risks in cyberspace, means to control them and responsibility for their own safety. Raising user awareness is extremely important, as it contributes to building a cybersecurity culture where users learn to be responsible for their own cybersecurity. That is why it is important to continue the existing awareness programmes, develop new programmes and encourage citizens to participate in these programmes.[775]

In 2022, Slovenia adopted the Digital Inclusion Act. It aims to increase understanding of responsible and secure use of digital technologies and promote citizens' digital skills. One of the measures implemented under the Act is a digital voucher (of EUR 150) for entitled citizens (also certain student groups) to buy a computer. Adults over 55 will receive the voucher after completing a basic course of digital skills, which includes a section on internet security.[776,777]

3.22.4. The definition of cyber citizen skills

The National Education Institute Slovenia (ZRSS)[778] supports teachers in the definition of students' digital competence development from kindergarten to high school by means of indicators helping teachers plan activities to develop digital competence. All 21 digital competencies from DigComp model are used to prepare indicators. A team of teachers working in one class can use indicators to coordinate who will develop the competence in each DigComp model and to what level and which digital competencies a particular class should have. Moreover, each school can adapt the indicators to their special situation.[779] All five competencies and their defined sub-competencies are used in Slovenia's national competence framework for students. A table called "DigComp po razherid" (DigComp by grade) (in Slovenian) contains the indicators that describe the digital skills of an individual.[780]

References

[746] The Republic of Slovenia, Digital Slovenia, *Digital Slovenia 2020 – Development Strategy for the Information Society until 2020*, Digitalisation of Slovenia by Intense and Innovative Use of ICT and Internet in all Segments of Society (2016).
[747] A personal communication to the researcher, 20/06/2022.
[748] The Republic of Slovenia, Digital Slovenia, *Cyber Security Strategy*, *Establishing a System to Ensure a High Level of Cyber Security* (2016), 10–11.
[749] The Republic of Slovenia, *Cyber Security Strategy*, 9–10, 13.
[750] "VARNI NA INTERNETU," accessed on 29 November 2022, https://www.varninainternetu.si/.
[751] "Safe.si," accessed on 29 November 2022, https://safe.si/.
[752] The Republic of Slovenia, *Cyber Security Strategy*, 5.
[753] A personal communication to the researcher, 05/07/2022.
[754] A personal communication to the researcher, 23/06/2022.
[755] "About SI-CERT," accessed 4 November 2022, https://www.cert.si/en/about-si-cert/.
[756] A personal communication to the researcher, 23/06/2022.
[757] A personal communication to the researcher, 23/06/2022.
[758] A personal communication to the researcher, 05/07/2022.
[759] A personal communication to the researcher, 23/06/2022.
[760] "Slovenian Safer Internet Centre," accessed on November 10, 2022. https://www.betterinternetforkids.eu/sic/slovenia.
[761] A personal communication to the researcher, 05/07/2022.
[762] The Republic of Slovenia, *Cyber Security Strategy*, 5–6.
[763] A personal communication to the researcher, 20/06/2022.
[764] European Commission, *Digital Economy and Society Index (DESI) 2022: Slovenia* (2022), 7, 16.
[765] "Better Internet for Kids Slovenia," accessed on July 8, 2022. https://www.betterinternetforkids.eu/sic/slovenia.
[766] A personal communication to the researcher, 05/07/2022.
[767] "Safe.si Aplikacije," accessed on September 6, 2022. https://safe.si/orodja/aplikacije.
[768] A personal communication to the researcher, 05/07/2022.
[769] A personal communication to the researcher, 5 July 2022.
[770] A personal communication to the researcher, 20/06/2022.
[771] A personal communication to the researcher, 07/07/2022.
[772] A personal communication to the researcher, 05/07/2022.
[773] "The European Cybersecurity Month 2022 Awards," *ECSM*, accessed on November 8, 2022. https://cybersecuritymonth.eu/awards.
[774] "Slovenia - Darko EN.m4v," accessed on November 29, 2022. https://cybersecuritymonth.eu/countries/slovenia/slovenia-darko-en.m4v.
[775] The Republic of Slovenia, *Cyber Security Strategy*, 13.
[776] A personal communication to the researcher, 07/07/2022.
[777]European Commission, *Digital Economy and Society Index (DESI) 2022: Slovenia* (2022), 6.
[778] "Zavod Republike Slovenije za šolstvo, About us," accessed on 29 November 2022, https://www.zrss.si/en/.
[779] European Commission, Joint Research Centre, Pujol Priego, L., Cabrera, M., Kluzer, S., et al., *DigComp into action, get inspired make it happen: a user guide to the European Digital Competence framework*, Punie, Y.(editor), Carretero, S.(editor), Vuorikari, R.(editor) (Publications Office, 2018), https://data.europa.eu/doi/10.2760/112945, 138.
[780] "DigComp po razredih," accessed on July 11, 2022. https://docs.google.com/spreadsheets/d/1I6fOc-D3KK945ZC5nMJDHaBDm2kNhpJ25Ucl1PPM2BE/edit#gid=1097700938.

3.23. Finland

ITU, Global Cybersecurity Index (GCI) 2020	22/182 (Global), 14/46 (Europe)
National Cyber Security Index (NCSI)	11/160 (24 October 2022)
The Digital Economy and Society Index (DESI)	1/27

3.23.1. Strategic cyber education and training policies

According to the Finnish Cyber Security Strategy 2019, Finland's goal is to be among the top experts in cybersecurity internationally. One of the strategic guidelines is: "Development of cyber security competence – everyday skills and top skills as cyber security safeguards." Each individual is considered an important cybersecurity actor, and the strategy highlights the importance of ensuring that everyone has sufficient capacity to operate safely in a digital environment. The idea is to improve the cyber competence and understanding of all actors in society. The Finnish Cyber Security Strategy is considered to complement the EU's Cyber Security Strategy. Measures to promote cybersecurity competence include strengthening of training programmes related to cyber and information security, software and application development, information networks and telecommunications in vocational education, universities of applied sciences and universities, and strengthening of the national system for training and exercising digital security as part of digital security training in the public administration. The latter aims to develop the skills of personnel in public administration, businesses and other stakeholders as well as of citizens.[781] The Implementation Programme for Finland's Cyber Security Strategy details the practical measures for achieving the set goals. However, the Implementation Programme was prepared before the latest strategy. To develop cyber competence, it suggests planning and carrying out exercises the aims of which include developing citizens' information and cybersecurity skills. Responsibility for training is assigned particularly to actors in the third sector, including the National Defence Training Association of Finland and the Finnish Association for the Welfare of Older Adults. The National Digital Security Week organised by Digital and Population Data Services Agency in cooperation with Ministry of Transport and Communications is also considered to provide citizens with more information. Finnish National Agency for Education is assigned responsibility for producing additional material for general and vocational education.[782] The Finnish Cyber Security Development Programme states that citizens' cyber competence must be brought to a high level. In addition to the above organisations, it suggests supporting voluntary cybersecurity communities and utilising their competence in the development of general cyber competence. The programme also says that a communication plan should be created to raise citizens' awareness on cybersecurity.[783]

Finland's digital compass is a roadmap for digital transformation up to 2030, guiding the digital development work in Finland. The cardinal points of the compass are skills, digital transformation of businesses, digital public services, and secure and sustainable digital infrastructures. The Government report: Finland's Digital Compass says: "Media literacy and the ability to tackle influence through information are, for their part, preconditions for a trust-based, open and democratic society." It is important to ensure that citizens possess the necessary skills, but strong digitalisation competence and education, and digital skills (which can be considered to include cybersecurity skills) are seen as Finland's strengths. Profiling as an expert in cybersecurity is seen as an opportunity for Finland. Current threats in Finland include especially cyber attacks, influencing through disinformation, data theft and identity theft. Cybersecurity should be included in all activities in the digital world, and the Compass states that each individual is responsible for security.[784]

3.23.2. The current state of cyber citizen skills education and training

Finland offers relatively lot of both formal education (part of official school curricula or education programmes) and unofficial education (other training programmes) in cybersecurity. The content of the education is not consistent even on the formal level, and the amount of received cybersecurity training depends largely on your own activity. E-learning material and training in cybersecurity is available for everyone on the Internet, but the problem is to reach citizens who need the training the most. Training courses are difficult to find, and everyone may not recognise their need for additional training. Groups that have a special need for training include seniors, young people, children and people working with children (children and young people are better placed because they receive cybersecurity education as part of their formal school education.) Adults may be left without training, if cybersecurity training is not offered at the workplace.[785,786] Cybersecurity training is offered in Finland but directed differently toward different age groups, both quantitatively and qualitatively. Finland's digital compass lists as one of the objectives that cybersecurity training is an integral part of the education and training offering at all levels of education, and citizens' cyber skills have improved.[787]

A study published by the University of Jyväskylä in 2022 has extensively mapped education and training of cybersecurity. Projects to develop cybersecurity training in primary and lower secondary education, such as the Cyber Security Development Programme and the New Literacies Programme, are currently running, i.e. teaching is under active development. At the moment, teaching of cybersecurity belongs especially to the "Information and communication technology" competence area but other competence areas also address topics relevant for building cyber citizen skills. For example, the comprehensive competence areas "Taking care of oneself, managing daily life" and "Multiliteracy" are essential for cybersecurity skills.[788] Upper secondary education also includes themes related to cybersecurity but the how and to what extent vary greatly depending on the organiser and education programme. The annual ITK Conference is a large digital education and learning event aimed at teachers of primary, lower secondary and upper secondary schools. The conference is important for the continuing education of teachers in cybersecurity.[789] Also, in Finland increasing the number of cyber experts is seen as important.[790]

Higher education degrees focusing cybersecurity are offered by universities of applied sciences and universities. At the moment, there are 15 degree programmes (8 Bachelor's degrees and 4 Master's degrees in universities of applied sciences, and 3 Master's degree programmes in universities), and new programmes are being planned. However, it must be noted that themes related to cybersecurity are included in several other higher education degrees.[791,792]

In Finland, adult education centres and libraries teach cybersecurity skills to different age groups, but the challenge is that this depends largely on the skills of the staff, and it must first be identified what should be taught. Training open for all is also offered by the HAUS Finnish Institute of Public Management Ltd, even though the main target group is the employees in central government. One of the largest providers of training for citizens is the National Defence Training Association of Finland (MPK) which organises plenty of cybersecurity courses at different levels both online and as contact teaching around Finland. Some of these courses are open for all, some are meant for reservists. In addition to the above, cybersecurity training for citizens is offered by the Women's National Emergency Preparedness Association, adult education centres and summer universities, libraries, the Finnish Association for the Welfare of Older Adults, Technology Industries of Finland, the Digital and Population Data Services Agency (DVV), the National Cyber Security Centre operating under the Finnish Transport and Communications Agency Traficom and KyberVPK, Victim Support Finland (RIKU) and other organisations related to cybersecurity.[793] Several cybersecurity games as well as websites and materials focusing on cybersecurity training are available in Finnish. The "This works!" technology education project offered by Technology Industries of Finland for first graders includes a cybersecurity module. It is a material package that teachers can order.[794] Together with the University of Jyväskylä, MPK has published a course called "Cyber Security for Every Citizen". It is aimed at everyone and does not require any previous skills. The course offers information and teaches skills required for secure behaviour in the digital world.[795] The Digital and Population

Data Services Agency (DVV) has produced a training module called "The Digitally Secure Life" which also includes a game. The aim of the training module is to teach secure behaviour in the digital world, especially for the personnel of various organisations.[796] "Spoofy" is a mobile game for primary school pupils. It teaches what to do if you meet bullies online.[797] The Finnish Public Service Media Company (YLE) has published a game called "Troll Factory" to illustrate influencing through information. In the game, the player sees how fake news, emotional content and bot networks are used to influence people.[798] YLE has also created "Troll Bunker", an escape room game where the player is a journalist who has been trapped by a misinformation-spreading internet troll. It focuses especially on fake news.[799]

The European Cybersecurity Month has been celebrated for several years in Finland in October, and the business community has been particularly active during the event. During this event, both public actors and many cybersecurity companies bring up cyber themes and arrange a wide array of different events and campaigns for their personnel and stakeholder groups. [800] In Finland, the National Cyber Security Centre has offered the most content for the general public. It has arranged events and produced material on the annual cybersecurity themes for citizens. In 2022, the material included videos with themes like ransomware and phishing.[801] DVV also arranges an annual Digital Security Week in October, aimed especially at different organisations.[802] In the interviews for this study, people shared their hopes and expectations for the Cyber Citizen project. The hopes included improving the level of citizens' cybersecurity skills but it was also stated that the level of cyber citizen skills is not really measured at the moment, and it was suggested that maybe the material produced in the Cyber Citizen project and the related outputs could be utilised to this end. People also hoped for continuity of the contents and the network produced during the project, including cyber citizen skills into existing entities and not presenting them as a separate topic, and attracting citizens' interest with benefits instead of scaring them with the risks.[803,804,805]

3.23.3. National characteristics

At the moment, the coordination of cybersecurity is dispersed but it is continuously developed.[806,807] The hacking of Vastaamo that became public in 2020 created a lot of visibility for cybersecurity threats and affected the population at large when the sensitive patient data of more than 30,000 people were stolen (however, citizens could not have done anything to prevent this incident). Also, the Russian attack on Ukraine and Finland's NATO membership process have shown the importance of digital security in relation to the intention to harm and damage between nations, increased the amount of news on cyber threats and attracted citizens' interest in the topic. Finns are active in the digital world, and society trusts different services and institutions. This trust also exists in the digital world, making it necessary to raise awareness on threats.[808,809] As in the above study on cybersecurity training[810], also this study came across the diversity in the related concepts and terms.[811]

3.23.4. Definition of cyber citizen skills

Even though cyber citizen skills have not been defined using this term, MPK, one of the largest training providers, says that "cyber security competence is becoming a new civic skill." [812] The study interviews found that cybersecurity cannot be outsourced any more but everyone should master the basics.[813] A study by the University of Jyväskylä listed awareness of threats and media literacy as cyber citizen skills.[814] DVV is currently working on the definition of digital competence and digital civilization, which also include security skills. The Digital Compass put out to hearing also acknowledges the need for a more detailed definition of digital skills (and cybersecurity skills) and says that we must move from basic technical skills towards a more versatile and deeper understanding of digital skills in the digital era. It lists "the evaluation of information sources, the identification of different motives and recognising misinformation and disinformation and having awareness with regard to online safety and security" as topical themes. [815]

References

[781] Secretary of the Security Committee, "Suomen kyberturvallisuusstrategia 2019," *Government resolution on October 3, 2019,* (Security Committee, 2019).
[782] Security Committee, *Suomen kyberturvallisuusstrategian toimeenpano-ohjelma 2017–2020* (Security Committee, 2017).
[783] Ministry of Transport and Communications and Rauli Paananen, "Kyberturvallisuuden kehittämisohjelma," *Liikenne- ja viestintäministeriön julkaisuja 2021:7* (Helsinki: Ministry of Transport and Communications, 2021).
[784] Ministry of Transport and Communications, "Valtioneuvoston selonteko – Suomen digitaalinen kompassi," *VNS 10/2022 vp* (Helsinki: Ministry of Transport and Communications, 2022).
[785] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* (Jyväskylä: University of Jyväskylä, Faculty of Information Technology, 2022), 11–12, 109–110.
[786] A personal communication to the researcher, 04/08/2022.
[787] Ministry of Transport and Communications, "Valtioneuvoston selonteko – Suomen digitaalinen kompassi".
[788] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 7, 20–22.
[789] "ITK2023," *ITK conference*, accessed on December 27, 2022. https://itk-konferenssi.fi/en/.
[790] In the recent strategy of the Finnish Information Security Cluster (FISC ry) for the years 2023–2025, one of the five main themes is increasing cyber competence by ensuring the availability of domestic and international experts and the smoothness of entry into the country. A personal communication to the researcher, 12/12/2022.
[791] "Oulun yliopisto vahvistaa kyberturvallisuuden osaajien koulutusta," *University of Oulu*, accessed on November 26, 2022. https://www.oulu.fi/fi/uutiset/oulun-yliopisto-vahvistaa-kyberturvallisuuden-osaajien-koulutusta.
[792] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 33–53, 88–89.
[793] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 93-94, 97-98.
[794] "Tämä toimii!," *Technology Industries of Finland*, accessed on July 30, 2022. https://tamatoimii.fi/.
[795] "Kansalaisen kyberturvallisuus," *University of Jyväskylä*, accessed on June 15, 2022. https://www.avoin.jyu.fi/fi/opintotarjonta/informaatioteknologia/kyberturvallisuus.
[796] "Digiturvallinen elämä," *Digital and Population Data Services Agency*, accessed on 3 August 2022, https://dvv.fi/digiturvallinen-elama.
[797] "Spoofy," *CGI Inc*, accessed on July 15, 2022. https://www.spoofy.fi/.
[798] "Trollitehdas," *The Finnish Public Service Media Company*, accessed on August 6, 2022. https://trollitehdas.yle.fi/.
[799] "Trollibunkkeri," *The Finnish Public Service Media Company*, accessed on August 7, 2022. https://yle.fi/aihe/artikkeli/2020/11/11/trollibunkkeri.
[800] A personal communication to the researcher, 19/12/2022.
[801] "Euroopan kyberturvallisuuskuukausi - European Cyber Security Month," *Traficom*, accessed on November 15, 2022. https://www.kyberturvallisuuskeskus.fi/fi/euroopan-kyberturvallisuuskuukausi-european-cyber-security-month.
[802] "Kutsu digiturvaviikolle," *Digital and Population Data Services Agency*, accessed on October 30, 2022. https://dvv.fi/-/kutsu-digiturvaviikolle-2022.
[803] A personal communication to the researcher, 04/08/2022.
[804] A personal communication to the researcher, 14/07/2022.
[805] A personal communication to the researcher, 19/12/2022.
[806] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti*, 110.
[807] A personal communication to the researcher, 04/08/2022.
[808] A personal communication to the researcher, 14/07/2022.
[809] A personal communication to the researcher, 19/12/2022.
[810] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 6.
[811] A personal communication to the researcher, 19/12/2022.
[812] "Kyber- ja informaatioturvallisuus," *MPK*, accessed on October 10, 2022. https://mpk.fi/koulutukset/kyber-ja-informaatioturvallisuus/
[813] A personal communication to the researcher, 14/07/2022.
[814] Lehto Martti, *Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimushankkeen loppuraportti,* 15.
[815] Ministry of Transport and Communications, "Valtioneuvoston selonteko – Suomen digitaalinen kompassi", *VNS 10/2022 vp* (Helsinki: Ministry of Transport and Communications, 2022).

3.24. Denmark

ITU, Global Cybersecurity Index (GCI) 2020	32/182 (Global), 19/46 (Europe)
National Cyber Security Index (NCSI) 24 October 2022	15/160 (24 October 2022)
The Digital Economy and Society Index (DESI, 2022)	2/26

3.24.1. Strategic cyber education and training policies

The Danish Government published the National Strategy for Cyber and Information Security in 2021. The strategy is for 2022–2024. With regard to educational policies, the strategy mentions the importance of teaching digital skills especially to children and young people to help them avoid becoming victims of cybercrime or digital fraud. As one of the key objectives, the strategy lists improving the digital literacy of children, young people and adults by implementing a variety of educational programmes in the field of education and training. The situation can also be improved by increasing awareness at all levels of education by interesting teaching material and events. Citizens' access to cyber and information security skills will be strengthened through adult education and training and further education. [816]

The national policy and guidance concerning cybersecurity is strongly founded on two strategies: the above national strategy for cybersecurity but also the common public digital strategy of the government, municipalities and regions. [817]

3.24.2. The current state of cyber citizen skills education and training

Sikkerdigital.dk is a national information portal established based on Strategy for Cyber and Information Security and the digitalisation strategy. The portal aims to ensure a high level of knowledge and competence of citizens, authorities and companies. It offers quizzes, advice, different guides on cybersecurity and campaign material. From a pedagogical perspective, it is not an educational website but rather an informative website. In Denmark, there are several public and private organisations which work with cyber civic skills. Key players include libraries, Cybernauterne, Ældresagen, Center for Digital Dannelse and the Danish Safer Internet Centre. The key problem for various actors has been that they have different goals for raising awareness on cybersecurity. Because of this, work is done without a joint coordinated network.[818]

The need for IT and media skills has been recognised starting from pre-school. The pre-school curriculum defines "IT and digital media" as part of the teaching, and children's awareness is increased with the help of games based on experimental practice and digital media. In pre-school, IT and media skills are divided into four learning perspectives: critical researcher, analysing receiver, determined and creative producer, and responsible participant.[819]

Information security and cybersecurity have not been defined separately in the national curriculum. They are generally referred to as digital skills. The curriculum does not include mandatory subjects related to digital skills. Instead, these skills should be integrated into all subjects. National tests and evaluations of students' learning results only give an indirect indication of their ICT competence. In 2018, the Ministry of Education of Denmark started a "Technological literacy" pilot both as a separate subject and as material integrated into other subjects. In the Danish primary and lower secondary school, digital competence is included in the national curriculum as a transverse subject (IT and media) which should be integrated into all subjects at all levels and in the common objectives of some subjects. As the name implies, it focuses on technology and communication. The themes of study units concentrate on ensuring that the pupils are able to manage different entities. These entities are

related to critical search and interpretation of different types of media, critical analysing and evaluation of their content and knowing how to use different tools in an ethical and self-assertive manner.[820]

A national initiative was made to strengthen the online skills of children and young people and in December 2021, the Danish Government signed an agreement with several political parties to strengthen children's and adolescents' ability to navigate in the digital world. The goal of the agreement was to establish units to support learning of the "digital traffic rules" for digital society. These are rules that everyone must know – from an early age. The initiatives cover primary, lower secondary and upper secondary school as well as vocational education. The most important initiatives are: "Digital Traffic Club" which concentrates on providing children and young people with information on how to become critical users of digital technology, and "school patrols for digital road safety" which aim to support healthy digital culture in schools.[821]

A chapter concerning upper secondary schools in Denmark says that educational institutions should offer opportunities and educational content for the development of students' digital skills. This also includes cyber skills. In upper secondary schools, this subject is called informatics. Students must be able to protect their digital identity and data online and be able to explain the technical and human aspects of IT security. Because Denmark has regular upper secondary schools, technical upper secondary schools and commercial upper secondary schools, informatics may either be a mandatory subject or an optional subject. It is optional only in technical upper secondary schools.[822]

Digital skills are addressed in all curricula for adult education and general adult education. The programmes consist of an extensive set of subjects. Digital skills are included in all curricula. The aim is to strengthen digital competence of individuals and coach learners for work and social life where fast technological development increases demand for digital competence. Since 2017, employed people have had the opportunity to complete digital courses essential for their work tasks. The content of the courses can be prioritised based on needs. [823]

In Denmark, most universities and higher education institutions offer teaching in cybersecurity. An overview of the offering shows that most education programmes emphasise the technical aspects of cybersecurity training, but, for example, the Copenhagen Business School offers a course oriented towards commercial cybersecurity. Universities offer a total of only four actual degree programmes in cybersecurity, two for a Master's degree and two for a Bachelor's degree.[824]

In Denmark, there are several websites aimed at citizens for improving their cyber knowledge and skills. These include the emu.dk website (Denmark's learning portal) which offers training courses to support focusing on cybersecurity and digital judgement in different subjects and at different levels[825], and the Cyber hub website which offers free courses in cybersecurity for interested citizens, amateurs and professionals. The content on this page is focused on technical competence.[826] The Sikker:Cyber website offers module courses on different cybersecurity topics for everyone from beginners to advanced users. The website has been developed by the IT University Copenhagen.[827] The Cyber Mission website has been created in coordination with the National Agency for IT and Learning. The platform offers a vocational course in cybersecurity.[828] The Danish Safer Internet Centre promotes a safer and better use of digital and social media among children and young people and prevents illegal and unwanted content concerning children and young people.[829] The Media Council for Children and Young People maintains a website aimed especially at children and adolescents which guides and shares information about the use of digital media.[830] "My digital Self-Defence" is an application offered for citizens by the Danish Consumer Council. It shares up-to-date information about threats in cyber world. The application also advices how to act if an accident happens and your information is stolen. You can download the application for both Android and Apple.[831] The Center for Digital Dannelse offers materials subject to a fee for teaching and learning about the phenomena in the digital world, mainly for children in the primary and lower secondary school. The website also contains plenty of advice for parents on how to teach these topics.[832] The Center for Digital Youth Care is Denmark's leading association providing digital advice for children and young people. It arranges workshops based on practical knowledge and lectures on digital wellbeing and pedagogics.[833] The Cyber Hub website focuses on helping young people in the digital space. On the website, you can choose what

you want to ask about, and the website produces answers for different situations. You can also send questions by email or SMS or ask another adolescent.[834] Coding Pirates is a non-profit organisation to develop children's technological courage with the help of inventiveness and creative force. It implements projects one of which is a game for learning about cybersecurity.[835]

In Denmark, information about cybersecurity has mainly been shared through publicly financed websites and information campaigns. Sikkerdigital.dk, a website aimed at Danish citizens, is a key forum for raising awareness on cybersecurity. The portal arranges annual public events related to cybersecurity.[836] Since 2013, the Danish Computer Security Incident Response Team (DKCERT) has prepared reports on citizens' information security. The covered topics are experiences, knowledge and behaviour.[837]

3.24.3. National characteristics

Denmark has a strong education system on preventive cyber skills which dates back to the decisions made at the end of 1990s to create two education structures: an Eastern and Western IT university. The Western IT University became a part of the Faculty of Technical Sciences at Aarhus University, and the Eastern one became a brand new university called IT University of Copenhagen.[838]

The Siri Committee, which maps the opportunities offered by artificial intelligence, published a report in 2019. According to the report, "a digital education programme should be prepared for the entire population, not just children and adolescents, based on learning, creativity and interactivity and activating all actors from libraries to folk high schools, civil society, medias and other stakeholder groups."[839]

Based on discussions with experts in different fields during the study, in the future, Denmark should invest in developing coordination between various actors. It seems that the actors at the core are the ones who play a key role in producing different cybersecurity campaigns and websites for citizens' needs. The Sikkerdigital.dk website aimed at citizens should be further developed to ensure that as many citizens as possible find it and receive information and tools for behaving securely in the digital world. It is also necessary to pay more attention to seniors in identifying threats in the digital world. The received responses also indicate that education and training should be reformed. Observations have shown that teaching that focuses mainly on technology is not enough to bridge the skills gap, but we also need experts who understand business in the digital world.[840]

3.24.4. The definition of cyber citizen skills

Based on the studied materials and received responses, Denmark has not defined the meaning of citizens' cyber citizen skills. Despite this, it is generally evident that citizens' cyber skills should be strengthened. Citizens should be able to act securely on the Internet and protect their own data. It can also be observed that the efforts concentrate on affecting citizens' competence by providing more information about the threats in the cyber world, not so much on teaching what to do in different situations. Different publications speak of increasing citizens' knowledge and skills but they do not specify what these skills are.

References

[816] The Danish Government, *The Danish National Strategy for Cyber and Information Security 2022–2024* (2021), 23–25.
[817] The Danish Government, *The Danish National Strategy,* 23–25; A personal communication to the researcher, 30 June 2022*;* "Sikkerdigital.dk," accessed on June 30, 2022. https://sikkerdigital.dk/.
[818] A personal communication to the researcher, 30/06/2022; "Sikkerdigital.dk," accessed on June 30, 2022. https://sikkerdigital.dk/.
[819] Børne- og Undervisningsministeriet, *Børnehaveklassen. Faghæfte 2019* (København K: Emu.dk, 2009), 75.
[820] A personal communication to the researcher, 12 June 2022; *It og Medier – Vejledning*, accessed on October 24, 2022. https://emu.dk/sites/default/files/2020-04/It%20og%20Medier%20-%20vejledning.pdf.
[821] A personal communication to the researcher, 10/08/2022 and 22/08/2022.
[822] A personal communication to the researcher, 5/07/2022.
[823] A personal communication to the researcher, 02/09/2022.
[824] "Study in Denmark, Find your Study Programme," *Danish Agency for Higher Education and Science*, accessed on July 12, 2022. https://studyindenmark.dk/portal.
[825] "EMU, Denmark's learning portal," accessed on July 14, 2022. https://emu.dk/.
[826] "Industriens Fond. Cyber Hub," accessed on August 12, 2022. https://cyberhub.dk/.
[827] "Sikker: Cyber," accessed on July 22, 2022. https://sikkercyber.dk/.
[828] "Cybermissionen," *Ministry of Education, Agency for IT and Learning; Cyber Skills*, accessed on August 10, 2022. https://cybermissionen.cyberskills.dk/.
[829] "Safer Internet Centre Denmark," *Sikkert Internet*, accessed on June 30, 2022. https://sikkertinternet.dk/english.
[830] "Om Medierådet for Børn og Unge," accessed on May 14, 2022. https://www.medieraadet.dk/.
[831] "Forbrugerrådet Tænk," accessed on August 23, 2022. https://taenk.dk/om-os/vores-apps.
[832] "Center for Digital Dannelse," accessed on July 10, 2022. https://digitaldannelse.org/.
[833] "Center For Digital Pædagogik," accessed on June 29, 2022. https://cfdp.dk/.
[834] "CyberHus," accessed on July 23, 2022. https://cyberhus.dk/.
[835] "Coding Pirates," accessed on September 22, 2022. https://codingpirates.dk/.
[836] A personal communication to the researcher, 02/07/2022 and 22/08/2022.
[837] DKCERT, *Danskernes informationssikkerhed* (The Danish Agency for Digitalisation, 2020).
[838] "Center for Information Security and Trust," *ITU CISAT*, accessed on 27 December 2022 https://cist.dk/.
[839] A personal communication to the researcher, 26/09/2022.
[840] A personal communication to the researcher, 24/05/2022, 06/06/2022 and 17/06/2022.

3.25. Czech Republic

ITU, Global Cybersecurity Index (GCI) 2020	68/182 (Global), 35/46 (Europe)
National Cyber Security Index (NCSI) 24 October 2022	5/160 (24 October 2022)
The Digital Economy and Society Index (DESI, 2022)	19/26

3.25.1. Strategic cyber education and training policies

The Czech government published the National Cyber Security Strategy in 2020. The strategy is for 2021–2025. The strategy takes a strong stand on including cybersecurity as part of all levels of the education system and across all fields. According to the strategy, it is important to start education at an early stage, at the pre-school level. The strategy emphasises training of educators in addition to pupils and students, as they play an important role in developing information literacy. The strategy also considers seniors, which is exceptional. Seniors are often one of the most vulnerable groups who are exposed to the negative effects of modern digitalisation. This group should be educated in recognising disinformation and in the safe use of digital technologies. With regard to other educational activities to improve cybersecurity, awareness will be increased by broadly or narrowly targeted awareness campaigns arranged by responsible actors, such as the state, private companies and academic non-profit organisations.[841]

The Cyber Security Strategy has been complemented with a separate action plan. To reach the defined goals, the action plan lists the following measures: preparing a national education plan in the field of cybersecurity, modernising primary and secondary school curricula to promote cybersecurity topics and digital competencies, and developing and maintaining an e-learning platform.[842] With regard to cybersecurity, the Policy Statement of the Government of the Czech Republic mentions supporting citizens' digital skills through education and training programmes. This applies to all generations.[843]

Cyber strategy is included in Strategy for the Education Policy of the Czech Republic where it is defined as part of digital competence in basic education. The National Cyber and Information Security Agency (NCISA, also known as NÚKIB) is responsible for the development of cybersecurity training on a strategic level. It cooperates with the Ministry of Education, Youth and Sport with regard to amendments of the Framework Educational Programme for Basic Education which include the strategy's educational requirements. However, NCISA is not responsible for the content of education. The schools are responsible for education programmes, and these must be based on the principles of the framework programme. The Ministry of Education, Youth and Sport addresses cybersecurity from two perspectives: security and prevention. Security includes schools' common secure computer network, and prevention focuses especially on arranging different conferences, webinars and courses. In cooperation with NCISA, the Ministry of Education, Youth and Sport calls for securing digital skills in the area of sharing and evaluating information but also in independent e-learning, managing pupils' credentials, and securing and uniting communication platforms.[844]

3.25.2. The current state of cyber citizen skills education and training

The educational content of cybersecurity has not been separately included in the Framework Education Programme for Preschool which defines the most important requirements, criteria and rules for institutional education of preschool children. However, the Czech Republic has already offered various activities and courses for preschoolers. Since 2022, the National Cyber and Information Security Agency (NCISA) has published applicable educational activities concerning secure Internet use.[845]

The basic education programme includes a section "Information and communication technologies" which contains teaching cybersecurity skills for citizens, including basic device management, information searches and identifying the reliability of information and interconnections. The framework programme document was modified in 2021 to meet the national need to offer better IT education for children, and digital skills were added at that time. At the proposal of the Ministry of Education, Youth and Sport, prevention of cyber threats and secure behaviour on the Internet were included in the education programmes. The factors and risks in certain areas should be considered in education. These include the world of Internet and its special characteristics, risk behaviour in cyberspace, copyright legislation, cyber piracy, digital identity, cyber harassment and online bullying.[846]

In 2016, the Ministry of Education, Youth and Sport and the pedagogical institute established the DigiKoalice platform. The platform unites schools with the ICT world in digital education and focuses on developing the digital skills of children and adults. Cybersecurity is one of the addressed topics. At the moment, an extensive reform of basic and upper secondary education is prepared based on the Strategy for the Education Policy 2030+. The reform focuses on secure working with digital technologies.[847]

In principle, seniors have been taken into account in the preparation of the National Cyber Security Strategy, but it did not reach the practical level until 1 October 2022 when NCISA's training unit published an online course it had developed. An extensive media campaign was launched in connection with the publication. The tool is called SENIOR. It aims to improve the personal security of ageing adults when using the Internet, and it is considered very useful in identifying harmful e-communication. Seniors have participated in the planning of the tool, making the published tool resemble a manual.[848]

You can earn a Bachelor's degree in cybersecurity in the Masaryk University. The Ambis College is running a three-year project to develop an innovative education programme in cybersecurity. The Prague Security Studies Institute also offers a Security Scholars Program, which includes studies in cybersecurity and digital security. Private institutions are also offering paid courses in cybersecurity. These include the Prague Coding School (Praha Coding School), NH Prague Knowledge Center and SANS DFIR Europe Prague.[849,850]

In the Czech Republic, there are several websites aimed at citizens for improving their cyber knowledge and skills. The training department of the National Cyber and Information Security Agency (NCISA) arranges courses, lectures and conferences for various target groups. These include the annual Festival of Secure Internet, as well as games and activities for children, such as Vanda & Eda and Digital footprint.[851] The key objective of the Cybercon BRNO Conference is to connect cybersecurity specialists in different fields to share information and experiences (last organised in September 2021).[852] The IS2 Information Security Summit (8 and 9 June 2022) grants the annual "The Hall of Fame Cybersecurity" award for people who have had a positive influence on cybersecurity in the Czech Republic.[853] The Qubit cybersecurity conference in Prague is an international conference. The ninth conference was arranged in 2022, and the event unites people interested in cybersecurity and cybersecurity training around the world.[854]

The Future of Cyber Conference is mainly about cyber awareness, cyber education and exchanging information and knowledge in the field of cybersecurity between various actors. The main organiser is NCISA together with the CzechCyber Center, the Ministry of the Interior and other partners, including higher education institutions.[855] Czech Cyberton offers cyber exercises for teenagers[856], and Internet Highway is an online game[857]. Interland is a game introducing the key aspects of online security. You get a diploma for completing the game.[858] NÚKIB has a learning portal which contains different courses in cybersecurity. Courses are also offered for citizens of different ages, schools and healthcare personnel. Especially the basic course in cybersecurity is aimed at citizens.[859] The Cz.niz Academie website offers users independent study courses, which mostly cover the technical basics.[860]

3.25.3. National characteristics

Based on interviews and the material, cyber citizen skills are considered important for citizens in the Czech Republic. It should be noted that seniors are already incorporated at the strategy level. It is interesting that the Czech State has been taking responsibility for training citizens in cyber skills. This has led to the creation of learning platforms, games, books and campaigns for different target groups. The Ministry of Education, Youth and Sport assumed a strong role in reinforcing digital skills and competence. The National Cyber and Information Security Agency (NCISA) is developing an educational platform which mainly concentrates on producing educational material for different target groups. However, an estimated time of completion was not available. In the Czech Republic, a special association called CZ.NIC is responsible for coordination at national level with the aim of improving children's online security in particular. The national Cyber Security Act assigns authorised institutions and bodies a key role, enabling them to influence the nation's cybersecurity and the efficiency of the entire system. Seamless cooperation between these actors and the private sector is essential for the operation of the entire system.[861]

In the Czech Republic, upper secondary schools are using Haxagon, a platform for practising cybersecurity aimed to support general IT education. The platform utilises gamification, such as different levels, badges, achievements and scoreboards. You can use the platform independently regardless of place or device.[862] Based on the received information, the aim of the National Cyber and Information Security Agency is to continue and expand inclusion of cybersecurity in two main areas of education. These are increasing cyber awareness to build a common information standard (training for all) and training of cybersecurity specialists to meet the demand on the labour market.[863]

3.25.4. The definition of cyber citizen skills

Based on the received responses, the Czech Republic considers using proper password settings, social planning, secure Internet connections and protection of digital devices as cyber citizen skills. Prevention is an important part of cybersecurity, i.e. what preventive measures should be considered to achieve secure online behaviour. The perspective should be considered in the definition of the content. For example, a legislative perspective, academic environment perspective or end-user perspective.[864]

References

[841] National Cyber and Information Security Agency, *National Cyber Security Strategy of the Czech Republic for the Period from 2021 to 2025* (2021), 18–19.
[842] National Cyber and Information Security Agency, *Action Plan for the National Cybersecurity Strategy for the years 2021 to 2025* (2021), 16–18.
[843] Government of the Czech Republic, *Policy Statement of the Government of the Czech Republic* (2022).
[844] A personal communication to the researcher, 28/08/2022 and 9/09/2022; Ministry of Education, Youth and Sport, *Strategy for the Education Policy of the Czech Republic up to 2030+* (2020).
[845] A personal communication to the researcher, 26/08/2022; "Nukib," accessed on August 27, 2022. https://osveta.nukib.cz/course/view.php?id=105.
[846] A personal communication to the researcher, 26/08/2022; "Nukib," accessed on August 27, 2022. https://osveta.nukib.cz/course/view.php?id=105.
[847] A personal communication to the researcher, 11/08/2022; Ministry of Education, Youth and Sport, *Basic Education*, 34–35.
[848] A personal communication to the researcher, 2/10/2022; "SENIOR proti internetovým padouchům?," *Nukib*, accessed on October 3, 2022. https://osveta.nukib.cz/course/view.php?id=140#section-0.
[849] "Cybersecurity," *Masaryk University*, accessed on 13 September 2022, https://www.muni.cz/en/bachelors-and-masters-study-programmes/26540-cybersecurity; "Cybersecurity fundamentals," *Ambis College*, accessed on October 14, 2022. https://www.ambis.cz/cybersecurity-fundamentals; "Cyber security Academy," *Prague Security Studies Institute*, accessed on 20 October 2022, https://www.pssi.cz/projects/16-cyber-security-academy.
[850] "Brno University of Technology," accessed on January 4, 2023. https://www.vut.cz/en/.
[851] "Education," *National Cyber and Information Security Agency*, accessed on 23 August 2022, https://nukib.cz/en/cyber-security/education/.
[852] "Cybercon Brno," accessed on August 6, 2022. https://www.cybercon.cz/eng/.
[853] "Is2," accessed on September 17, 2022. https://is2.cz/en/.
[854] "Qubit Conference," accessed on October 24, 2022. https://prague.qubitconference.com.
[855] "Future of Cyber Konference," accessed on July 22, 2022. http://future-forces-forum.org/events/default/74_future-of-cyber-fcd?lang=cs.
[856] "Czech Cybertron," *Network security monitoring cluster*, accessed on January 4, 2023. https://www.czechcybertron.cz.
[857] ˇPedagogicka faculta, Univerzita Palackého v Olomouci," accessed on October 22, 2022. https://www.pdf.upol.cz/nc/pl/zprava/clanek/nova-online-hra-vznika-na-pdf-up-a-zaky-zakladnich-skol-uci-jak-se-bezpecne-chovat-na-internetu/.
[858]"Interland. Be internet awesome," accessed on June 15, 2022. https://beinternetawesome.withgoogle.com/cs_cz/interland.
[859] "NÚKIB," accessed on 17 May 2022, https://osveta.nukib.cz/local/dashboard/.
[860] "CZ.NIC Moodle," *Cz.nic Akademie*, accessed on December 20, 2022. https://moodle.nic.cz/.
[861] National Cyber and Information Security Agency, *National Cyber Security Strategy of the Czech Republic* (2020) 8, 18–19; "CZ.NIC," accessed on September 18, 2022. https://www.nic.cz/; National Cyber and Information Security Agency, *Legislation* (2022), accessed on September 10, 2022. https://nukib.cz/en/cyber-security/regulation-and-audit/legislation/; A personal communication to the researcher, September 14, 2022.
[862] A personal communication to the researcher, 19/09/2022 and 26/08/2022.
[863] A personal communication to the researcher, 09/09/2022.
[864] A personal communication to the researcher, 25/08/2022 and 26/08/2022.

3.26. Hungary

ITU, Global Cybersecurity Index (GCI) 2020	35/182 (Global), 22/46 (Europe)
National Cyber Security Index (NCSI) 2022	35/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	22/27

3.26.1. Strategic cyber education and training policies

In its Cyber Security Strategy 2013, Hungary emphasises awareness raising as a means to improve national cybersecurity and focuses especially on private users and SMEs. Attention is also paid to developing training at different levels of education and courses for training and professional development of civil servants. In education, cybersecurity should be integrated into IT education. Children are in a privileged position. They should be protected with the help of awareness and other measures. Strategic cooperation is carried out with universities and research institutes which participate in cybersecurity research and development.[865] The update of the cybersecurity strategy 2018 (Strategy on the security of network and information systems) is to promote education, research and development programmes and increase security awareness. The Cyber-Security Academy of the National University of Public Service contributes to the arranging of cybersecurity training and continuing education as well as the coordination of education and research activities related to the security of cyberspace and the related resources. Hungary actively organises domestic forums and campaigns and actively participates in international cybersecurity awareness forums and campaigns (such as ECSM, the European Cybersecurity Month). Hungary's objective is to use education, research and development opportunities offered by cybersecurity to create a competitive domestic knowledge base which is in line with international practices and meets the needs of the domestic labour market. Hungary's digital education strategy sets the objectives and measures for developing digital competence and awareness to promote information security and developing education and fields of vocational training.[866] The next update of the cybersecurity strategy is expected to be completed at the end of 2023.[867] Hungary's digital programme (DJP, Digitális Jólét Program 2030) is a comprehensive long-term project helping Hungary to prepare for changes brought by digitalisation in everyday life, business life, economy and at social level. People are at its core, and the Government of Hungary prepares citizens and companies for digitalisation with the help of the DJP programme. DJP2030 creates a strategic framework for digital policy for 2021–2030. It is an overarching strategy that covers, for example, the Digital Child Protection Strategy of Hungary (DCP) and the Digital Education Strategy of Hungary (DES), which is built around the four main pillars of the EU's Digital Decade Compass, measured by DESI, one of which is digital skills. [868,869]

3.26.2. The current state of cyber citizen skills education and training

For school children, cybersecurity training is part of the educational content of primary and lower secondary school. However, this topic has not been given much emphasis. In primary and lower secondary education, pupils complete the International Computer Driving Licence (ICDL, formerly known as ECDL[870]) and the related basics of cybersecurity. Tens of thousands of children a year also use Google study material. In Hungary, the Safer Internet project funded by the EU is managed by an NGO in the field. In universities, students gain basic skills in cybersecurity as part of IT education and in special courses in the field. For the general public, campaigns are offered in social media and the internet. The National Cyber Security Center for Hungary (NCSC, Nemzeti Kibervédelmi Intézet) implements communication projects aimed at the general public. There is no educational content about cybersecurity for special groups, and a project aimed at seniors did not materialise.[871] According to ENISA's CyberHEAD database, cybersecurity is taught in Hungary in the National University of Public Service.[872]

The Eötvös Loránd University (ELTE) offers a Master's degree in IT where you can also specialise in cybersecurity.[873,874]

In Hungary's new curriculum (2020/2021), a subject called informatics (Informatika, curriculum 2012) will be gradually changed to digital culture (Digitális Kultúra), which is a mandatory subject for grades 3–11 (8–17-year-olds). With this change, the content will be modernised to include new topics. Digital culture teaches everyday skills required in information society, such as basic digital skills, problem-solving skills, digital literacy, creative and secure use of digital equipment and users' informed attitude from the perspective of an individual, community and society. Based on the curriculum, children start to learn digital culture in grade 3, but it has an important role in the development of the learning process on previous grades, 1 and 2 (for example use of digital education material and digital literacy in class).[875,876]

The Hungarian Safer Internet Centre (SIC), which is part of the EU's Better Internet for Kids programme (BIK), promotes a safer use of the internet and mobile technologies among children and young people (and through them also adults). Young people participate in events, such as the Safer Internet Day (SID) and Children's Day, help to disseminate online material about more secure Internet use, listen to courses and help to develop educational material. Young people also discuss real problems in their online lives and share ideas in meetings. Surf Safely lessons are taught in schools and libraries, for example. They address important topics related to everyday life, such as protecting your personal data, cyberbullying, netiquette, passwords and digital footprints. The interactive lessons contain short videos and easy exercises, whereas a more critical approach is applied to parents and teachers. Many of the trainers are volunteers. They are experts in the field, such as employees in IT companies.[877,878] The website also contains Google study material, such as the Interland game which teaches the principles of digital security[879], and other educational material for children and adolescents, for example, a book on the dangers of the internet and social networking, and material for parents, including videos and the Mongu mobile application for managing children's smartphones.

More and more organisations participate in the European Cybersecurity Month every year, but the pandemic made it challenging and in 2021, the National Cyber Security Coordinator (NCSC) emphasised arranging of events that have gone well for years. NCSC also arranged events focusing on younger public because that helps to reach a larger target group (for example parents, friends and teachers).[880] Also, many of the campaigns in Hungary in 2022 were aimed at young people (pupils and students) or professionals. With regard to campaigns arranged by companies, one example are the events organised by Bosch Hungary's IT department for its personnel. Kibertámadás! podcast is a campaign aimed at all Hungarians.[881] Under the child protection programme, more aware internet use is part of the "Tudatosabb internethasználat" campaign which offers young people themed videos on controversial and risky phenomena in the online environment. The topics discuss addiction, cyberbullying, disinformation, fake news and body image problems.[882] "Gyerekkel a digitális világban" is aimed at parents and includes five short modules on the basics of digital child protection and education. The addressed topics include children's privacy and personal data online, conscious 'media diet', screen time and addiction.[883] The child protection programme also includes an online mentor programme for age-mates and Sango picture book for 5–9-year-olds for discussing risky situations with parents. The National Media and Infocommunications Authority (NMHH) has established Magic Valley Media Literacy Education Centres (Bűvösvölgy médiaértés-oktató központokat) where 9–16-year-olds can learn media literacy. Internet workshops discuss topics such as privacy, sexting and bullying, and teach how to identify useful websites and applications.[884] The "Gyerek a neten" programme (Young people on the internet) and Internet hotline are also part of the campaigns offered by NMHH. So is the NETRE FEL programme which encourages seniors in digital learning through their inner circle. Seniors mostly receive support from their children or grandchildren and their loved ones. People also listen to advice given by loved ones, making them valuable helpers setting a useful example because it is important to teach seniors secure use of digital devices.[885]

In Hungary, there is a need for a centralised website on cybersecurity issues. For example, none of the Ministries are responsible for general awareness raising at the moment. Campaigns and educational material could be

created especially with EU funding. The cybersecurity theme should be given more prominence through media to attract the attention of the general public. Measures should be targeted especially at seniors because they form a risk group, particularly in terms of disinformation and online fraud. The Centre of Excellence for Countering Hybrid Threats does good work, but concrete results have not yet been achieved in Hungary. The EU is currently preparing cybersecurity legislation, and its importance should be explained to the general public as well. ENISA could assume a role in this effort. The European Cybersecurity Month is well known in Hungary but the fact that it is an EU project should be made more visible.[886]

3.26.3. National characteristics

In Hungary, children and their protection are an important part of fostering national cybersecurity culture, and Hungary has a separate strategy for children: The Digital Child Protection Strategy of Hungary, adopted in 2016. Hungary wants to maintain and develop a child-friendly cybersecurity environment. This is supported with the objectives of the European Better Internet for Kids (BIK) strategy. Under this strategy, high-quality online content is created for children and young people and awareness raising is supported. Hungarian NGOs with competence on protecting children online play an important part in this work.[887]

The Smart Kindergarten Program, Okosóvoda, started in 2018 as part of the child protection programme. Since then, hundred kindergartens a year are entitled to free website services for three years. The programme includes a part called “DigiMini” intended for studying pre-schoolers’ smart device user behaviour, attitudes and rules of media at home and at the kindergarten and to assess the practice and attitudes of preschool teachers. According to the study results, 80–90 per cent of kindergarten children use smart devices daily. Half of pre-schoolers are familiar with the benefits and possible dangers of the internet. Parents and kindergarten teachers are not prepared for digital parenthood or education. Half of kindergarten teachers object to the use of digital devices. According to pre-primary education teachers, it is the parents’ responsibility to teach the children to use smart devices. Based on the study results, Smart Kindergarten 2.0 Program will be developed, especially to include preschool teachers’ education and empowerment.[888]

3.26.4. The definition of cyber citizen skills

Hungary is developing a Hungarian DigKomp for Citizens system, which is part of Hungary's DJP programme, based on the European DigComp model (DigComp 2.1, which will be updated to 2.2.). The model is dynamic, i.e. it is updated on a continuous basis. The system model will be created into a tool for the purpose of developing and evaluating citizens’ digital skills. The system includes DigKomp Office, a free and open for all DigKomp Learning Platform (with a topic/material and tutorial bank), Digital Training Register and DigKomp Certificate Centers. The target group of the platform’s learning environment ranges from school-age children to working people and senior citizens. Knowledge, skills, and attitude are adapted to proficiency levels, task types and templates. The model has five competence areas based on the DigComp model. In Hungary, the “Communication and collaboration” competence area includes online shopping and use of digital services (communication) as well as digital identity competence (for example using Netflix creates a digital footprint). Citizen Basic describes the necessary level of digital competence required in everyday life and Citizen Plus shows the proficiency level required in working life and higher education. With regard to basic civic skills, information and data literacy are important skills as well as security competence, but creating digital content is not as important in everyday life. That is the level that senior (and all other) citizens should reach. The Plus level emphasises communication, cooperation and security competence.[889,890,891]

References

[865] Viktor Orbán, Prime Minister, MAGYAR KÖZLÖNY, *Magyarország Nemzeti Kiberbiztonsági Stratégiájá* (6338-6341) Official Journal of Hungary N:o 47 (March 2013), 6341.
[866] "A hálózati és információs rendszerek biztonságára vonatkozó Stratégia," accessed on October 24, 2022. https://nki.gov.hu/wp-content/uploads/2020/11/Strat%C3%A9gia-a-h%C3%A1l%C3%B3zati-%C3%A9s-inform%C3%A1ci%C3%B3s-rendszerek-biztons%C3%A1g%C3%A1ra.pdf.
[867] A personal communication to the researcher, 13/06/2022.
[868] "About Digital Success Program," accessed on October 27, 2022. https://digitalisjoletprogram.hu/en/about.
[869] European Commission, *Digital Economy and Society Index (DESI) 2022: Hungary* (2022).
[870] "Digitális érettségi a társadalomnak: új feladatokat kapott az ECDL/ICDL," accessed on November 29, 2022. https://njszt.hu/hu/news/2022-06-28/digitalis-erettsegi-tarsadalomnak-uj-feladatokat-kapott-az-ecdlicdl.
[871] A personal communication to the researcher, 13/06/2022.
[872] "CYBERHEAD – Cybersecurity Higher Education Database," *ENISA*, accessed on November 27, 2022. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=hun.
[873] "ELTE Eötvös Lórand University," accessed on November 27, 2022. https://www.elte.hu/en/computer-science-msc.
[874] "CYBERWISER.eu, Hungary (HU)," accessed on November 27, 2022. https://www.cyberwiser.eu/hungary-hu.
[875] MAGYAR KÖZLÖNY, *MAGYARORSZÁG H I VATALOS LAPJA, H I VATALOS*, N:o 17, (31 January 2020), 427-428.
[876] European Commission, / EACEA / Eurydice, *Informatics education at school in Europe*, Eurydice report (Luxembourg: Publications Office of the European Union, 2022), 37, 100.
[877] "Hungarian Safer Internet Centre," accessed on November 28, 2022. https://www.betterinternetforkids.eu/sic/hungary.
[878] "A biztonságos internetezés kulcsa," *Saferinternet*, accessed on November 28, 2022. https://saferinternet.hu/.
[879] "Legyél az Internet Ásza!," *Saferinternet*, https://saferinternet.hu/legyel-az-internet-asza.
[880] ENISA, *European Cybersecurity Month (ECSM) 2021* (2022), 109.
[881] "Cybersecurity Activities, Hungary," *ECSM 2022*, accessed on October 7, 2022. https://cybersecuritymonth.eu/activities?containsDate=&country[]=HU&endDate=&perPage=10&reqPage=2&searchText=&sortOrder=ascending&startDate=October%204%2C%202022.
[882] "Tudatosabb internethasználat," *DGYS - Magyarország Digitális Gyermekvédelmi Stratégiája*, accessed on 28 November 2022, https://digitalisjoletprogram.hu/hu/tartalom/tudatosabb-internethasznalat.
[883] "Gyerekkel a digitális világban," accessed on November 28, 2022. https://digitalisgyermekvedelem.hu/gyerekkelonline.
[884] "Hands-on workshops to promote the conscious use of media, Magic Valley Media Literacy Education Centre," accessed on November 28, 2022. https://magicvalley.eu/.
[885] "Szupersegítő leszek!," *NETRE FEL, NMHH-program*, accessed on November 28, 2022. https://netrefel.hu/segitoknek.
[886] A personal communication to the researcher, 13/06/2022.
[887] Orbán, *Kiberbiztonsági Stratégiájá*, 6341.
[888] "Smart Kindergarten Program, Okosóvoda," (EN), accessed on November 28, 2022. https://digitalisgyermekvedelem.hu/okos-ovoda.
[889] "30.03 The development of the Hungarian DigKomp System to assess and improve the digital competence of citizens," accessed on November 25, 2022. https://all-digital.org/events/the-development-of-the-hungarian-digkomp-system-to-assess-and-improve-the-digital-competence-of-citizens/.
[890] "The development of the Hungarian DigKomp System to assess and improve the digital competence of the citizens," accessed on November 25, 2022. https://telecentreeuropeaisbl.sharepoint.com/sites/AllDIGITAL-PublicforExternalSharing/Shared%20Documents/Forms/AllItems.aspx?id=%2Fsites%2FAllDIGITAL%2DPublicforExternalSharing%2FShared%20Documents%2FWEBSITE%2FAD%20WEEKS%202022%20PRESENTATIONS%2F30%2E03%20Hungarian%20DigiKomp%2FDigKomp%5FWebinar%5Ffinal%2Epdf&parent=%2Fsites%2FAllDIGITAL%2DPublicforExternalSharing%2FShared%20Documents%2FWEBSITE%2FAD%20WEEKS%202022%20PRESENTATIONS%2F30%2E03%20Hungarian%20DigiKomp&p=true&ga=1.
[891] "30.03 The development of the Hungarian DigKomp System," accessed on October 26, 2022. https://www.youtube.com/watch?v=tgP9BC_ahRQ.

3.27. Estonia

ITU, Global Cybersecurity Index (GCI) 2020	3/182 (Global), 2/46 (Europe)
National Cyber Security Index (NCSI) 2022	4/160 (24 October 2022)
The Digital Economy and Society Index (DESI) 2022	9/27

3.27.1. Strategic cyber education and training policies

Estonia's Cybersecurity Strategy has been prepared in 2018. Its objectives include promoting a cyber-literate society which requires raising cybersecurity awareness among citizens, state and private sector. All citizens active in cyberspace are responsible for developing cybersecurity skills. In the educational system, cybersecurity is addressed at all levels of education as part of developing digital competencies. It is important to keep students' and teachers' cybersecurity component skills in digital competency models up to date, not forgetting the measuring of skills. The Cybersecurity Strategy emphasises the importance of preventive actions. It is necessary to talk about the prevailing risks to the general public and provide advice for mitigating risks. Different agencies must cooperate to raise the general public's awareness of cyber threats and measures to be taken after a possible attack.[892]

3.27.2. The current state of cyber citizen skills education and training

In Estonia, development of digital competence is managed by the Education and Youth Board Harno (Haridus- ja Noorteamet, HARNO), operating under the Ministry of Education and Research.[893] Since 2020, the development of cybersecurity education has been determined by the DigComp framework[894], which must be followed in all Estonian schools.[895] The evaluation criteria of the DigComp framework's Safety competence area have been described generally and also specified for all levels of general education, starting from kindergarten.[896] Schools provide optional IT classes depending on their resources. There are no mandatory IT classes. Cybersecurity is taught in connection with IT classes from primary school to upper secondary school.[897]

Curricula and material for teaching cybersecurity is available for grades 1–6 and grades 10–12. Only a curriculum is available for pupils in grades 7–9. With regard to the optional "Informatics" subject, there are preliminary descriptions of the content for cybersecurity education.[898] For example, secure use of passwords and identifying suspicious links is taught in grades 1–3. Topics in grades 4–6 include security of digital communication and management of digital identity, intervening in cyberbullying and protecting computer equipment. Pupils in grades 7–9 learn about identifying and responding to the most common threats, cybersecurity acts and regulations, protecting digital identity, using e-services and safety and ethics of online discussions.[899] An e-course called "Küberkaitse" ("Cyber defence")[900] fulfils the criteria for upper secondary education (grades 9–12) and contains more complicated topics.[901] More emphasis is placed on e-services and legislation than with younger pupils. Students also learn how to identify different types of online frauds and protect computer equipment.[902]

There is a separate motivation model for teaching cybersecurity in the school system. Schools can evaluate their success themselves or request an external evaluator. The motivation model also helps students to evaluate their digital security competence.[903] In tertiary education, you can study cybersecurity in two different Master's programmes. The Tallin University of Technology (Tallinna Tehnikaülikool, TalTech) offers a Master's programme called "Cybersecurity" with the University of Tartu (Tartu Ülikool).[904] An international Master's programme, Cyberus Erasmus Mundus Master in Cybersecurity, is managed by the University of South Brittany (Université Bretagne Sud). TalTech is responsible for part of the teaching in this programme.[905]

TalTech and Estonian schools cooperate to raise pupils' and students' cybersecurity awareness. PhD candidates specialising in cybersecurity at TalTech visit schools to talk to children about Internet security.[906] School education is also complemented by an extracurricular programme, Smartly on the web (Estonian Safer Internet Centre), and the related projects.[907] The Estonian Information System Authority (Riigi Infosüsteemi Amet, RIA) coordinates raising cybersecurity awareness in Estonia. It gathers information about the level of citizens' cybersecurity awareness and organises activities based on the results.[908] RIA maintains "Ole IT-vaatlik"[909], a portal which aims to teach how to use the Internet and smart device more securely. The portal has separate sections for work users, regular users and parents, and you can test if your behaviour in the cyber world is secure. RIA regularly arranges awareness campaigns to improve Estonia's cybersecurity.[910] Most of the training for citizens is related to the digital identity card. (In Estonia, every citizen must have a digital identity card for using bank services and voting, for example.)[911] For example, in connection with the 2021 election, RIA arranged a campaign online about the safety of voting and shared videos and infographics in Facebook and Twitter.[912] The campaign in 2019 was targeted at over 55-year-olds and their inner circle. The campaign highlighted the meaning of cyber hygiene.[913] *RIA's incident response department* CERT-EE aims to prevent risk situations related to cybersecurity and to reduce security risks. CERT regularly arranges various events and information campaigns and issues warnings and notifications to users about security flaws identified in Estonian systems and applications.[914]

Different education centres, folk high schools and culture centres offer unofficial paid training courses which also include cybersecurity topics.[915] For example, citizens can learn about secure use of the Internet and its services, password management and authentication.[916] The Estonian Unemployment Insurance Fund (Eesti Töötukassa) offers free labour market training for the unemployed. It also offers IT courses and training on cybersecurity.[917]

The Estonian Police has so-called web officers who answer citizens' cybersecurity questions submitted online. Also third sector NGOs, such as the Estonian Union for Child Welfare (Eesti Lastekaitse Liit), contribute to training.[918] In addition, active Estonian volunteers teach seniors how to use the digital identity card, Facebook and email, for example.[919]

There are several opportunities for self-studying. For example, NATO's Cyber Defence Awareness e-Learning course aims to enhance the general user's awareness of cybersecurity risks and measures to mitigate those risks.[920] A company called *CybExer Technologies* has designed self-study material "My Cyber Hygiene", which has been translated into 12 languages.[921] In addition to the above, the University of Tartu offers self-study courses that are open for all, some of which address cybersecurity. It should be noted that cybersecurity is often included in the teaching of digital skills. For example, digital courses offered in libraries have provided tips for password management, etc.[922]
Communication companies coordinate some cybersecurity campaigns. For example, Telia has conducted a campaign for children to prevent cyberbullying.[923] Annual campaigns include the EU's Safer Internet Day and the European Cybersecurity Month (ECSM). Safer Internet Day's programme has included webinars for professional educators and gathering teaching material for kindergarten teachers.[924]

Self-study material, contests and quizzes for different target groups (children and adolescents, parents and teachers) are available on the Safer Internet Centre's portal.[925] It offers children videos and tips on Internet use as well as a game called Spoofy. For young people, it provides information about the security of smart devices and social media, and cyberbullying. Teachers can use the learning material and lesson plans provided in the portal in their work. An interactive game for young people called "Nastix ja turvalline Internet"[926] includes tasks related to privacy, identifying viruses and security of mobile devices. The portal also contains more challenging tasks for advanced users concerning encrypting and logical inference, for example.[927,928]

3.27.3. National characteristics

The cybersecurity culture in Estonia can be described with the word transparency. For example, people have quite quickly adopted the SMARTID technology related to the digital identity card. They also trust the Government managing this technology.[929] To measure the level of citizens' cyber hygiene, Statistics Estonia (Eesti statistika) conducts an annual query, "Information technology in the household", for 16–74-year-old permanent residents and the members of their households. In recent years, the cyber hygiene level of the Estonian population has increased but there is still room for improvement. For example, people become victims of phishing or lose control of their digital service by clicking wrong links[930]. Seniors' level of cyber hygiene is clearly lower than that of younger people.[931] On the other hand, a study aimed at young people found out that more challenging cybersecurity issues are problematic for young people as well. Also, their attitude towards security often leaves room for improvement.[932] One challenge schools are facing is a shortage of motivated and competent teachers who are able to teach cybersecurity integrated with other curricular topics.[933] Another shortcoming is that cybersecurity is not a mandatory subject in the curriculum, and teaching it in schools is often left for one person.[934]

With regard to teaching the basics of cybersecurity, Estonia is extending this to younger and younger age groups, and it is recommended teaching starts already in kindergarten.[935,936] Young people are attracted to the field of cybersecurity through various competitions (for example CyberPin, CyberDrill, CyberCracker and CyberSpike). Cyber Battles, coordinated by CTF Tech, have gained international popularity. They are cybersecurity training and competition events for young people, but the company also has its own e-learning platform which is open and free for all interested individuals. Teachers can use online material and games in school lessons.[937] Research revolving around cybersecurity education is active in Estonia. Strong players include the University of Tartu and Taltech which is running an interesting gamification project called "Cyber security awareness and prevention game for schools".[938,939]

3.27.4. The definition of cyber citizen skills

DigComp's Digital Competence Model is a framework which defined cyber citizen skills in Estonia and must be applied to teaching in all schools.[940] The interviews included in this study showed that when teaching is targeted at regular citizens, it is important to learn about password management and privacy. Other important aspects include authentication and deliberation when deciding which links to click.[941] It should be emphasised to citizens that cybersecurity is not a goal, but an enabler. In other words, you need to take care of security when you want to do something. Highlighting caution in disclosing your personal data is also essential.[942]

References

[892] Republic of Estonia, *Cybersecurity strategy 2019-2022* (Ministry of Economic Affairs and Communications, 2019), 15, 64, 66–67.
[893] "The Education and Youth Board Harno," *European Union digital skills & Jobs Platform*, accessed on 3 November 2022, https://digital-skills-jobs.europa.eu/en/organisations/education-and-youth-board-estonia-harno.
[894] A personal communication to the researcher 25/06/2022.
[895] A personal communication to the researcher 05/12/2022.
[896] A personal communication to the researcher 25/06/2022.
[897] A personal communication to the researcher 20/06/2022.
[898] A personal communication to the researcher, 08/06/2022.
[899] Haridus- ja noorteamet, *Lisa 10: Valikõppeaine Informaatika, Tööversioon 19 May2022* (2022), 3–4, 6–7, 9–10, https://oppekava.ee/wp-content/uploads/2022/06/Lisa-13-PROK-Lisa-10-Valikoppeaine-Informaatika.pdf
[900] "Küberkaitse," *Ministry of education and research of Estonia*, accessed on November 3, 2022. https://web.htk.tlu.ee/digitaru/kyberkaitse/front-matter/introduction/.
[901] A personal communication to the researcher 20/06/2022.
[902] Haridus- ja noorteamet, *Lisa 9: Valikõppeaine Informaatika, Tööversioon 19 May 2022* (2022), 7, https://oppekava.ee/wp-content/uploads/2022/05/Lisa-26-GROK-Lisa-9-Valikoppeaine-Informaatika.pdf.
[903] Lorenz Birgy, "Cybersecurity education and competitions in Estonia," *Tallinn University of Technology,* accessed on 3 November 2022, https://docs.google.com/presentation/d/15d-OGUUNe5IbuBkT_agiVBkT0fHI-F4wa-LE_xAWLeU/present#slide=id.p1.
[904] "MSc in cybersecurity," *Tallinn University of technology*, accessed on January 4, 2023. https://taltech.ee/en/cyber-msc.
[905] "Cyberus Erasmus Mundus Master in Cybersecurity," *ENISA*, accessed on January 4, 2023. https://www.enisa.europa.eu/topics/education/cyberhead/#/programme/858795598eed4fe5981803cbfae817bf?programme=Cyberus%20Erasmus%20Mundus%20Master%20in%20Cybersecurity.
[906] ENISA, *Raising Awareness of Cybersecurity A Key Element of National Cybersecurity Strategies* (ENISA, 2021), 14.
[907] A personal communication to the researcher 08/06/2022.
[908] ENISA, *Raising Awareness of Cybersecurity,* 14–15.
[909] "Ole IT-vaatlik," *Riigi Infosüsteemi Amet,* accessed on November 3, 2022. https://www.itvaatlik.ee/.
[910] Republic of Estonia Information system authority, *Cyber security in Estonia 2021* (Tallinn: Information system Authority, 2022), 5.
[911] A personal communication to the researcher 21/06/2022.
[912] ENISA, *European Cybersecurity Month (ECSM) – Deployment report 2021* (ENISA, 2022), 103.
[913] Republic of Estonia, *Cyber security in Estonia 2021*, 32–33.
[914] "CERT-EE," *Information system Authority*, accessed on November 3, 2022. https://www.ria.ee/en/cyber-security/cert-ee.html.
[915] "Koolitused," *IT Koolitus*, accessed on November 4, 2022. https://koolitus.ee/koolitused.
[916] "Infoturve," *IT Koolitus*, accessed on November 4, 2022. https://koolitus.ee/teemad/infoturve.
[917] "Training search," *Eesti töötukassa*, accessed on November 3, 2022. https://www.tootukassa.ee/et/koolitused?keyword=cyber&pageSize=20.
[918] ENISA, *Raising Awareness of Cybersecurity*, 14.
[919] A personal communication to the researcher 21/06/2022.
[920] "Cyber defence awareness," *The NATO Cooperative Cyber Defence Centre of Excellence*, accessed on October 5, 2022. https://ccdcoe.org/training/cyber-defence-awareness-e-course/.
[921] "Estonian Cyber Security Company Provides Free Cyber Hygiene e-Learning in 12 Languages," *CYBEXER TECHNOLOGIES*, accessed on 4 November 2022, https://cybexer.com/news/estonian-cyber-security-company-provides-free-cyber-hygiene-e-learning-in-12-languages/.
[922] A personal communication to the researcher 20/06/2022.
[923] ENISA, *Raising Awareness of Cybersecurity*, 41.
[924] "Estonian Safer Internet Centre - Smartly on the Web," *European schoolnet*, accessed on November 4, 2022. https://www.saferinternetday.org/in-your-country/estonia.
[925] "Tärgalt Internetis," *Estonian Union for Child Welfare*, accessed on November 3, 2022. https://www.targaltinternetis.ee/en/.
[926] "Nastix ja turvalline Internet," *The Tiger Leap Foundation*, accessed on November 3, 2022. https://www.targaltinternetis.ee/nastix/.
[927] A personal communication to the researcher 21/06/2022.
[928] "Küberturbe Ülesanded," *Estonian Union for Child Welfare,* accessed on November 3, 2022. https://ylesanded.targaltinternetis.ee/index.html.
[929] A personal communication to the researcher, 21/06/2022.
[930] A personal communication to the researcher 20/06/2022.
[931] Republic of Estonia Information system authority, *Cyber security in Estonia 2022* (Tallinn: Information system Authority, 2022), 42.
[932] Lorenz Birgy, Kaido Kikkas and Kairi Osula, "Development of children's cyber security competencies in Estonia", *International Conference on Learning and Collaboration Technologies* (Springer: Cham, 2018), 7–8.
[933] Republic of Estonia, *Cybersecurity strategy 2019–2022, 68.*
[934] Birgy Lorenz, Kaido Kikkas and Kairi Osula. *Development of children's cyber security competencies in Estonia.* International Conference on Learning and Collaboration Technologies. Springer, Cham, 2018, 2, 8.
[935] A personal communication to the researcher, 21/06/2022.
[936] "Cyber security education in Estonia: from kindergarten to NATO Cyber Defence Centre," *Republic of Estonia Ministry of education and research*, accessed on November 4, 2022. https://e-estonia.com/cybersecurity-education-in-estonia-from-kindergarten-to-nato-cyber-defence-centre/ .

[937] "Cyber battle of Estonia," *CTF Tech*, accessed on November 4, 2022. https://www.ctftech.com/events/cyber-battle-of-estonia-2022/.
[938] A personal communication to the researcher 20/06/2022.
[939] A personal communication to the researcher 10/06/2022.
[940] A personal communication to the researcher, 05/12/2202.
[941] A personal communication to the researcher 20/06/2022.
[942] A personal communication to the researcher 21/06/2022.

4. Teaching cyber citizen skills in the European Union through gamification

4.1. Introduction to the study and the topic

Several ways have been produced in the European Union to develop citizens' cyber competence. Teaching cyber citizen skills is crucial in the modern society, and several EU countries have tried to make products and services available to the citizens. However, it is difficult to evaluate accurately how successfully the transmission of knowledge and teaching have improved national cyber skills.

This part of the report looks at educational games teaching cyber citizen skills. It places particular emphasis on the educational aspect and gamefulness of these games and addressing cybersecurity in teaching. The study only looks at games and learning environments produced by single, internationally renowned actors. The report also considers products from smaller actors as part of the whole. However, main emphasis is on data based on the ten largest and most comprehensive educational games.

The study only includes educational games targeted at EU countries. To narrow down the number of educational games to ones that best fit the context, games were excluded if they did not meet the following criteria: The games included in this study must be produced by reputable sources established in one of the EU countries. The game itself must be acknowledged by an operator established in the EU. The game must also be up to date, meaning that the content must still be relevant in the context. The games included in the study must be perceived as educational games. This means that they must have a clear learning goal and appropriate content to reach this goal. Educational games reviewed in this report must also be intended for EU citizens. The content must be neutral and have no political agenda, etc.

4.2. Criteria for comparison of research data

This study concentrates on reviewing and comparing educational games mainly in three areas. It also considers how well the games fit the target group, either at national or international level. To analyse each area and the games, distinct parameters are required for comparison and study purposes. The criteria used for analysing educational games have been selected based on previous studies focusing especially on the evaluation and analysis of the study games. [ANNEX 1] Even though the three areas used in the comparison of educational games in this study have been listed separately, there is clear correlation between them and the successful implementation of the games.[943,944,945]

Table 3: A list of educational games reviewed in the study.

Name of the game	Developer	Developer (country)	Target group
Cyber Chronix	The European Commission	EU	Children
Cyber Crime Time	IMC	Germany	Adolescents, adults
CyberKid	CANDI	Greece	Children, adolescents
Digitally Secure Life	DVV	Finland	Adults (/employees)
eFollowMe	Cyprus Pedagogical Institute of Ministry of Educational, Culture, Sports and Youth	Cyprus	Adolescents
EveryDay	Göteborg Sivukonttori, Ikämiessuojeluskunnan Säätiö	Finland	Adolescents, adults
Hackend	INCIBE	Spain	Companies(/employees)
Hackers vs. Cybercrook	INCIBE	Spain	Children, adolescents
Happy Onlife	The Joint Research Centre (JRC) of the European Commission	EU	Children
Juego Cyberscouts	INCIBE	Spain	Children, adults
Cyber Security Escape Room	University of Helsinki, Technology Industries of Finland	Finland	Adolescents
Nastix	Url OÜ, BadBlock	Estonia	Children
SecNum Académie	ANSSI	France	Adolescents, adults
Spoofy: A cyber game	IT service provider CGI together with the Finnish Transport and Communications Agency Traficom and the Finnish Climate Fund (formerly known as Vake Ltd.)	Finland	Children
Tacos	CASES.LU	Luxembourg	Adolescents, adults

4.2.1. Gamefulness

With regard to gamefulness, the focus was on the solutions made in the development phase of the educational game, selected based on known parameters in game development. These included gameplay, storification, user experiences and stories, course of the game, level of difficulty and design. Another important aspect of gamefulness is the layout of the game, i.e. everything that is visible to the user, from the design to usability. The

characteristics of educational games include especially gameplay, the course and structure of the game, difficulty level and development. This study does not focus on actual back-end solutions or choices because their direct impact is immaterial in this context. All games are either browser-based or applications that can be downloaded to a smartphone. The game platform did not affect the study.[946,947,948]

4.2.2. Game logic

In the analysis of the logic of educational games, the games mainly represented a logic based on one route or alternative solutions. The implementation of the games differed slightly in terms of selections, but typically the games could be routinely played through at different levels of difficulty and variation.

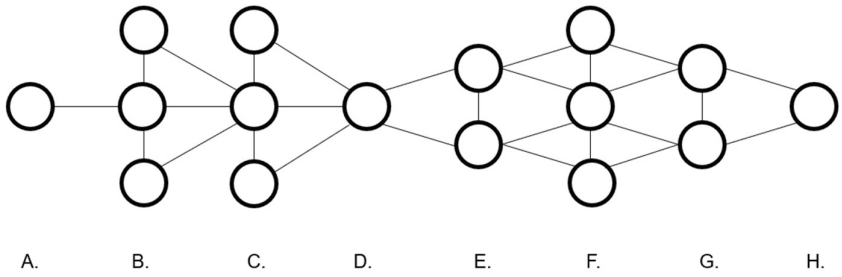

Figure 3: Typical logic of progress in educational games.

4.2.3. Teaching power

In the evaluation, emphasis is placed on teaching power and the pedagogic aspect of the game. The parameters used for analysing teaching power have been selected from other studies on educational games. The parameters are based on commonly known pedagogic results. Several factors affect the success of educational games, but only the most relevant parameters have been considered in this study. In this study, parameters most relevant for measuring the success of educational games include motivation of the user, emotions, goals, interactiveness, methods and feedback. The structure of the game, course of the game and how it is adapted based on the choices made and learning play an important role in making learning more effective.[949,950,951,952]

4.2.4. Cybersecurity and how it is taught

The scope, accuracy and target group of a national or international game teaching cybersecurity are important factors for producing a high-quality and functional educational game. It is important that the game provides a clear general overview of cybersecurity and the related factors, regardless of the user's baseline skills. Secure online activities, threats related to email and phishing and malware should also be addressed comprehensively. Passwords and their security should also be included in secure behaviour in the digital environment. Disinformation and influencing through disinformation are also an important part of understanding cybersecurity.[953]

4.2.5. Games in the EU context

One important criterion for educational games intended for EU citizens is how well the game fits the target group. Efficient and successful teaching of a large target group is difficult because users' baseline skills and background can vary significantly. Educational games should be proportionate to the desired context.

4.3. Study results

High quality of educational games is essential to ensure that the user is able to learn the lesson at least as well as by more traditional teaching methods. In this study, the objective was to learn about and review educational games teaching cybersecurity produced in the EU and aimed at EU citizens. The study focused only on educational games produced by acknowledged actors, and emphasis was placed on more comprehensive and holistic products. Based on comparison, the games were studied using proven criteria used in previous studies and their results. In principle, the study results show the differences in the quality of educational games, making it difficult to differentiate between single factors.

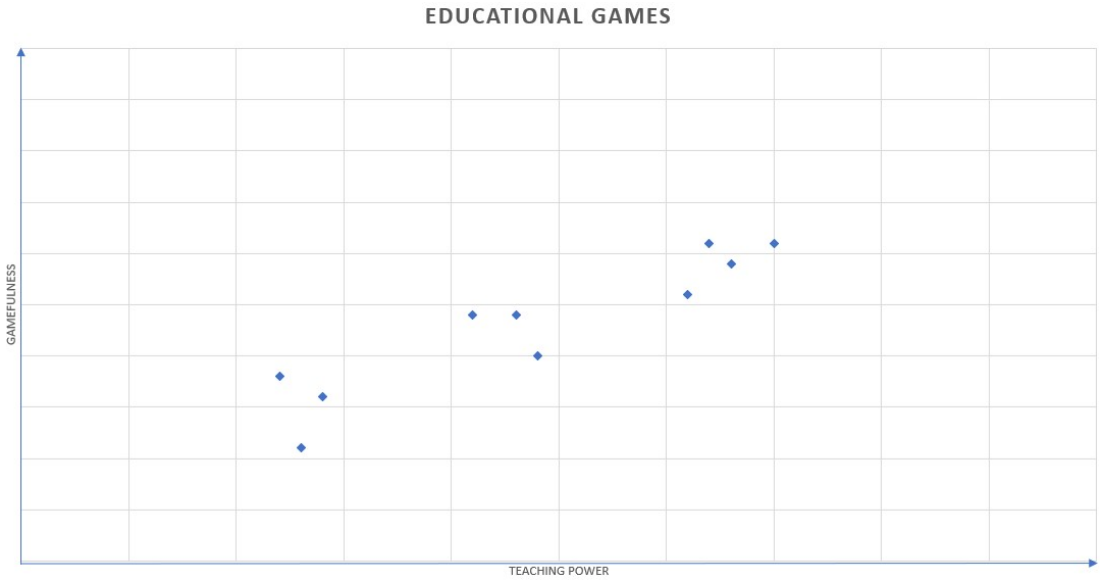

Figure 4: The diagram shows the correlation between the gamefulness of the educational games in the sample and the extent of the educational content. More detailed scoring can be found in Appendix 2. Not all games could be scored because of geographical (the game could not be downloaded from Finland) or language (the games could be played in Finnish, English and French) constraints.

The study results showed significant variance in the quality of game elements. In high-quality games, the lessons were integrated into elements known in the game industry. This was most evident in the review of storytelling and user journey. One good example of a successful educational game that is meaningful for the users is Cyber Crime Time produced by IMC. It fits the target group well, both visually and in terms of storytelling, and clearly lays out the basics of the lesson.

However, in some games learning was left on the backburner because of the gamification solutions. Based on the study results, it is difficult for the producers to find a good balance between gamefulness and the quality of education. In the majority of the reviewed games, the progress process clearly emphasised either learning or game elements but rarely succeeded in emphasising both.

There was also a significant variance in the pedagogic aspects of the reviewed games. In some of the games, the formation of user stories and journeys clearly shows from the start that the emphasis is on teaching power. Overlooking gamefulness, SecNum Académie, a MOOC based learning platform of the French National Agency for the Security of Information Systems (ANSSI), is a good example. Learning is efficient and materials are readily available, but the learning platform intentionally lacks game-like elements.

However, the teaching power of many games that focus on gamefulness is significantly below this level. Differences in the quality of the games can be divided into smaller subgroups in which this phenomenon is

more evident. Overall, it can be said that both gamefulness and teaching power correlate positively in the group of reviewed games. This can be explained by general differences in quality: poor game quality makes teaching difficult, and vice versa.

In the majority of educational games, the topic of cybersecurity is addressed comprehensively and from many perspectives. The topic becomes familiar regardless of the baseline level, but not even the educational games aimed at adults or organisations advance beyond a certain point. In other words, the reviewed games mostly offer comprehensive but low-level basic skills. None of the reviewed games teach skills beyond the basic level.

Another important criterion in the assessment of the success and quality of educational games is the target group. Based on the reviewed games, it can be said that games aimed at a very large target group are rarely as successful as games aimed at a very restricted target group. Spoofy produced by CGI is a good example of an educational game that works for the target group. Starting from the development stage, the interests of the target group (primary school children) have been considered both in the visual outlook and the user stories. It is easier to provide teaching at a suitable level for individual target groups, such as children, young people or an organisation's employees.

4.4. Reflection

Cybersecurity is a topical issue, and it would be critical to raise national competence to the required level. To this end, training and teaching should be provided starting from children and adolescents. Education should be continued and competence continuously maintained because cybersecurity plays a key role in organisations' threat imaginary. There are still several shortcomings in most of the educational games analysed in this report. However, it is positive to note that the EU is willing to invest in the development of digital teaching methods, both nationally and internationally. At the moment, disappointingly little has been done at a national level to teach cybersecurity skills through educational games. You would think that there would be a ready platform for learning a skill so critical to modern society which developers could use to monitor national development and competence. As online working gained an established status during the pandemic, it should speed up progress to other virtual learning platforms, including educational games. Developing and teaching cyber citizen skills should play a much bigger role in the European Union.

References

[943] Esther Oprins, Gillian van de Boer-Visschedijk, Maartje Roozeboom, Mary Dankbaar, Wim Trooster and Stephanie Schuit, "The game-based learning evaluation model (GEM): Measuring the effectiveness of serious games using a standardised method," *International Journal of Technology Enhanced Learning* 7 (2015), doi: 10.1504/IJTEL.2015.074189
[944] Marcelo Barbosa, Andreza Rêgo and Igor De Medeiros, "HEEG: Heuristic Evaluation for Educational Games," *Proceedings of SBGames 2015* (Federal Institute of Education, Science and Technology of Rio Grande do Norte, Brazil, 2015).
[945] Segomotso Mosiane and Irwin Brown "Factors Influencing Online Game-Based Learning Effectiveness," *The Electronic Journal of Information Systems Evaluation* Volume 23 Issue 1 (2020).
[946] Katharina Emmerich and Mareike Bockholt, "Serious Games Evaluation: Processes, Models, and Concepts," *Entertainment Computing and Serious Games* (2015).
[947] Alejandro Calderón and Mercedes Ruiz, "A systematic literature review on serious games evaluation: An application to software project management," *Computers & Education*, Volume 87 (2015).
[948] Narda Alvarado and Konstantin Mitgutsch, "Purposeful by Design? A Serious Game Design Assessment Framework," *Foundations of Digital Games 2012, FDG 2012 - Conference Program* (2012).
[949] Hanif al Fatta, Zulisman Maksom and Mohd Zakaria, "Systematic literature review on usability evaluation model of educational games: playability, pedagogy, and mobility aspects," *Journal of Theoretical and Applied Information Technology*, 96 (2018): 4,677–4,689.
[950] Alice Mitchell and Carol Savill-Smith, *The use of computer and video games for learning* (London: LSDA, 2004).
[951] Patricia Armstrong, *Bloom's Taxonomy* (Nashville: Vanderbildt University Center for Teaching, 2010).
[952] Akseli Huhtanen, *Verkko-oppimisen muotoilukirja – Käytännön työkaluja laadukkaan verkko-oppimisen muotoiluun* (Aalto University, 2019).
[953] Reneé Röpke and Ulrik Schroeder, *The Problem with Teaching Defence against the Dark Arts: A Review of Game- based Learning Applications and Serious Games for Cyber Security Education* (2019).

Annexes

Annex 1: List of criteria.

Name of publication	Publishers	Year of publication	Parameters selected from the source
Factors Influencing Online Game-Based Learning Effectiveness	**Segomotso Mosiane, Irwin Brown**	2020	Efficiency of educational games, feedback, concentration/immersion, flow
The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education	**René Röpke, Ulrik Schroeder**	2019	Teaching cybersecurity, learning with games, risk awareness
A systematic literature review on serious games evaluation: An application to software project management	**Alejandro Calderon, Mercedes Ruiz**	2015	Evaluation of educational games, assessment of software development
The game-based learning evaluation model (GEM): Measuring the effectiveness of serious games using a standardised method	**Oprins, E., Visschedijk, G., Roozeboom, M.B., Dankbaar, M., Trooster, W., Schuit, S.C.E**	2015	GEM, evaluation parameters
The use of computer and video games for learning	**Alice Mitchell, Carol Savill-Smith**	2004	Goals, interactions, feedback, adaptability, storytelling, user experience, social learning

A Motivational Model of Video Game Engagement	**Andrew K. Przybylski, C. Scott Rigby, Richard M. Ryan**	2010	
Assessing the Core Elements of the Gaming Experience	**Eduardo H. Calvillo-Gámez, Paul Cairns, and Anna L. Cox**	2010	
Serious Games Evaluation: Processes, Models, and Concepts	**Katharina Emmerich, Mareike Bockholt**	2016	Effectiveness and suitability of educational games, learning, behaviour, learning results
Validation of a mobile game-based assessment of cognitive control among children and adolescents	**Hyunjoo Songl, Do-Joon Yi, Hae-Jeong Park**	2020	
Systematic literature review on usability evaluation model of educational games: playability, pedagogy, and mobility aspects	**Hanif Al Fatta, Zulisman Maksom, Mohd Hafiz Zakaria**	2005	Usability, evaluation/feedback, playability, M-GBL, game pedagogics, heuristic evaluation
A systematic literature review of empirical evidence on computer games and serious games	**Thomas M. Connolly Elizabeth A. Boyle, Ewan MacArthur, Thomas Hainey, James M. Boyle**	2012	
Verkko-oppimisen muotoilukirja – Käytännön työkaluja laadukkaan verkko-oppimisen muotoiluun	**Akseli Huhtanen**	2019	Memory, motivation, attentiveness, emotions, design process, core content analysis
Bloom's Taxonomy (Vanderbilt University Center for Teaching)	**Armstrong, P.**	2010	Bloom's Taxonomy
Introducing the game design matrix: a step-by-step process for creating serious games	**Aaron J. Pendleton**	2020	MDA, DDE, LM-GM
Using User Created Game Reviews for Sentiment Analysis: A Method for Researching User Attitudes	**Björn Stråat, Harko Verhagen**	2017	
State of the art in Game Based Learning: Dimensions for Evaluating Educational Games	**Rabail Tahir, Alf Inge Wang**	2017	

HEEG: Heuristic Evaluation for Educational Games	**Marcelo B., Barbosa Andreza B., Rêgo Igor de Medeiros**	2015	A heuristic research model for educational games
Purposeful by Design? A Serious Game Design Assessment Framework	**Narda Alvarado, Konstantin Mitgutsch**	2012	Game design assessment-framework

Annex 2: List of game scores.

TEACHING POWER		SCALE 1–5									
Name of the game	**Games**	**Memory**	**Motivation**	**Attentiveness**	**Emotions**	**Feedback**	**Goals**	**Methods**	**Interactions**	**Educational material and its use**	**TOTAL:**
Happy Onlife	Game 1	3	2	2	2	3	3	3	2	3	23
Hackend	Game 2										NOT EVALUATED
Hackers vs. Cybercrook	Game 3										NOT EVALUATED
Juego cyberscouts	Game 4										NOT EVALUATED
CyberKid	Game 5										NOT EVALUATED
eFollowMe	Game 6										NOT EVALUATED
Tacos	Game 7	3	2	2	2	2	3	4	2	4	24
SecNum Académie	Game 8	4	3	2	2	5	4	4	2	5	31
Cyber Crime Time	Game 9	3	4	4	3	5	4	4	3	5	35
Digitally secure life	Game 10	3	3	3	4	5	4	4	3	4	33
Cyber security escape room	Game 11	2	1	1	1	2	1	1	2	1	12
EveryDay	Game 12	2	2	3	2	3	3	2	2	2	21
Spoofy: A Cyber game for children	Game 13	3	4	3	4	4	3	4	3	4	32
Nastix	Game 14	2	1	1	1	2	2	1	2	1	13
Cyber Chronix	Game 15	1	2	2	1	2	2	2	1	1	14

GAMEFULNESS		SCALE 1–5									
Name of the game	**Games**	**Gameplay**	**Storytelling**	**User experience**	**Adaptability**	**Structure**	**Design**	**Suitability to the target group**	**Flow**	**Immersion**	**TOTAL:**
Happy Onlife	Game 1	3	2	3	2	3	2	3	3	3	24
Hackend	Game 2										NOT EVALUATED
Hackers vs. Cybercrook	Game 3										NOT EVALUATED
Juego cyberscouts	Game 4										NOT EVALUATED
CyberKid	Game 5										NOT EVALUATED
eFollowMe	Game 6										NOT EVALUATED
Tacos	Game 7	2	1	2	2	3	3	3	2	2	20
SecNum Académie	Game 8	2	2	3	2	4	3	4	3	3	26
Cyber Crime Time	Game 9	4	5	4	2	3	3	4	3	3	31
Digitally secure life	Game 10	4	4	4	2	3	4	3	2	3	29
Cyber security escape room	Game 11	2	2	2	2	2	2	2	2	2	18
EveryDay	Game 12	3	3	2	2	3	2	3	3	3	24
Spoofy: A Cyber game for children	Game 13	4	3	4	2	3	4	5	3	3	31
Nastix	Game 14	2	1	2	1	1	1	1	1	1	11
Cyber Chronix	Game 15	3	2	2	1	2	1	2	1	2	16

5. Defining the content of cyber citizen skills

The EU's economic structures, cyberspace and the increasing diversity of the threat imaginary create a need for the definition and continuous development of cyber citizen skills. Improving cyber citizen skills has a direct effect on the security of the EU's critical infrastructure and digital economy. Good cyber citizen skills improve individual and social security and resilience.

At the request of the European Commission, this project identified concrete cyber citizen skills which promote adopting of the DigComp framework in the Member States. Gamification and digital learning portal have been selected as means to develop identifiable know-how. Developing cyber citizen skills has an extensive effect on security in the different dimensions of critical infrastructure, namely the political, economic and technical dimension (Critical Infrastructure Protection model, CIP).[954]

Cybersecurity aims to safeguard the electrical, IT, knowledge and network environment through various dimensions. Security is built by foresight, education, identification, prevention and preparing for the effects of disturbance in various dimensions on the critical functions of the environment. Cybersecurity thinking combines the preventive aspect, competence building, attitudes, information security, continuity management and preparedness aspects concerning the entire environment.[955]

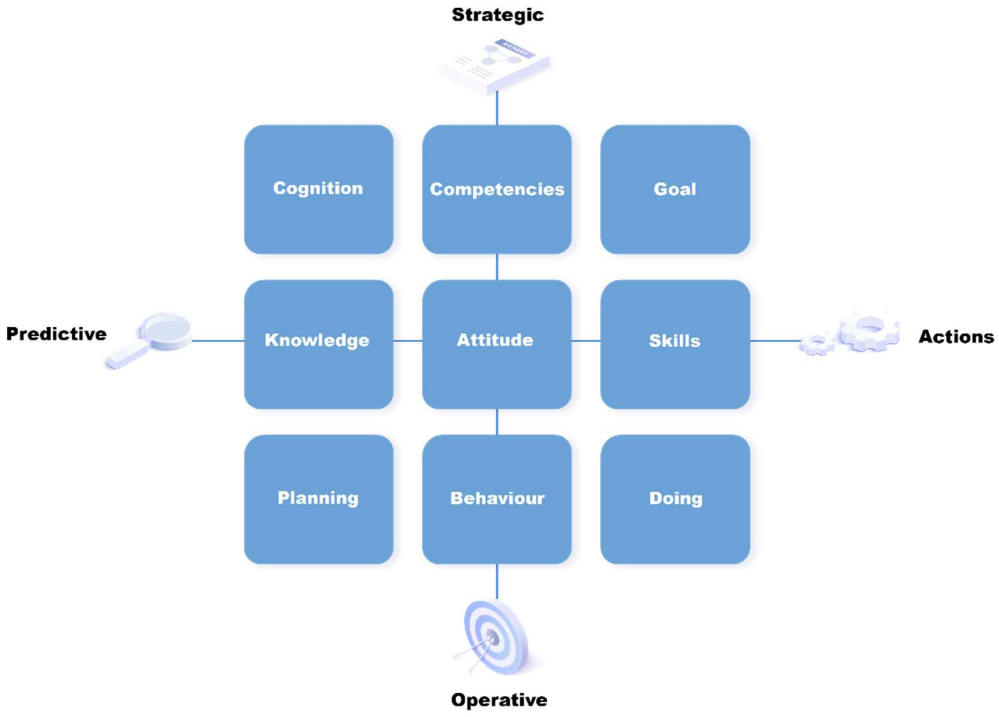

Figure 5: Framework for the classification of cyber citizen skills. At the heart of cyber citizen skills is attitude.[956]

With regard to learning cybersecurity, knowledge and skills should be reviewed in parallel to attitudes which influence motivation – citizens' attitudes are critical endpoints in terms of cybersecurity. Citizens' attitudes are based on personal and general images, benefits (environmental, social and economic sustainability), the ability

to influence and cybersecurity roles. Society plays a key role in the development of future attitudes and competence.

5.1. Cyber citizen skills

According to the research group's definition, a cyber citizen is a person who permanently or temporarily lives or resides in an EU Member State and uses digital services or directly or indirectly benefits from the provision of such services. The knowledge, skills and abilities required to operate in a cyber environment are jointly called cyber citizen skills.

Cyber citizen skills consist of factors which facilitate personal development and maintaining knowledge and skills to ensure that individuals have sufficient abilities and motivation to exercise deliberation in different situations. Cyber citizen skills mean bearing personal and social responsibility and understanding the importance of this responsibility for cyberspace.

1) Cyber citizens understand the significance of norms and rules as well as their rights and responsibilities.
2) Cyber citizens think critically and have a critical attitude towards events and available information.
3) They have know-how that helps them to understand what is valuable to each party in each situation.
4) Cyber citizens recognise the impact of their thinking and emotions in different situations.
5) They understand the basic principles of the technologies they use and know how to use them securely.

Figure 6: A citizen first encounters the Internet and moves on to understanding the systemic whole.

5.2. Developing cyber citizen skills to support the DigComp framework

The Digital Competence Framework for Citizens (DigComp 2.2) includes more than 250 examples of knowledge, skills and attitudes that help EU citizens use digital technologies confidently, critically and securely.

The framework guides definition and development of skills related to digitalisation in the European Union. Several national programmes are ongoing to implement the framework under the internal guidance and management of the Member States.[957]

5.2.1. Competence goals for cyber citizens

Cyber citizens should master different knowledge and skills required for secure behaviour in different life situations. The DigComp framework guides building understanding, competence and capabilities related to digitalisation at EU level. The required competence goals in future cyberspace should be studied in a larger framework and assessed in terms of individual and social resilience, sovereignty and wellbeing. Competence goals for cyber citizens are defined below based on mapping methods of new information, including a design method and a mapping literature review. The goals include knowledge and skills that can be developed through gamification and a digital learning portal.

5.2.1.1. Information and data literacy

Is able to evaluate the reliability of information and information sources

Evaluation of an information source depends on several factors from national culture to personal social environment and identity. In assessing the reliability, situation awareness skills and general understanding of the environment have a significant impact on decision-making and behaviour.

Is able to analyse, compare and process information

The know-how required for analysing information is individual and depends on the situation. Information from different sources may be contradictory and prepared for different purposes. A cyber citizen must be able to critically assess how the information is formed, where does it come from, on what forum and how it is presented, what are the background motives for producing the information, who produced it and to what purpose and what is the motivation. When processing information, cyber citizens use prevalent and chosen technology to ensure that information is processed and managed in a systematic and appropriate manner.

Understands the cyber environment

The environment consists of user experience and the hidden, more extensive social dimension of systems. In cyber environment, very few service or applications are truly free of charge. Browsers collect user information for marketing and product development purposes. It is important that cyber citizens understand the business logic behind services and applications and are aware that many factors affect search results and recommended content in social media.

Develops foresight skills

Understands how to develop knowledge and skills to improve foresight skills related to cybersecurity. Is able to choose learning and education programmes which develop foresight skills. Has an extensive understanding of the importance of preventive actions in terms of cybersecurity and system-level security.

5.2.1.2. Communication and collaboration

Understands rules and their impact on a personal and communal level

There are numerous rules, conditions of use and pieces of legislation to guide cyberspace, at both EU level and Member State level. These norms affect us on personal and social level. Increasing understanding of the existing regulations improves citizens opportunity and ability to abide by general rules.

Understands the effect of their actions on general security

Understands how the way they use a service or technology or process information can either improve or impair total security. Understands their responsibility and knows what to do in incidents or problem situations.

Manages their digital footprint

Understands the basic principles of the systematic operation of websites, cookies and systems. Is able to use the selected services and devices in such a way that harmful visibility and exposure is minimised.

Recognises the importance of different interaction channels in communication

Is able to select communication channels based on the needs and the content of the message. Understands that social media platforms can differ in terms of content, language, culture and technological solutions.

5.2.1.3. Digital content creation

Understands copyright principles

Understand how immaterial rights affect what content found online can be used, modified, cited and distributed and how. Is able to check and choose elements and information for content production that do not infringe the rights of others. Is able to protect their own copyrights. Asks for advice when problems or risks related to information security or data protection are suspected.

Knows how to use current technologies and services

Understands the main principles of used services and selected technologies to ensure that their activities do not threaten, intentionally or unintentionally, existing content or information security.

5.2.1.4. Safety

Is able to use prevalent technology securely

Understands the main principles of used and selected technologies, knows how to change their settings when necessary and analyse the included content and information. Is able to use selected off-the-shelf software responsibly. Has a general understanding of what factors have the most impact on the security of used technologies and applications. Is able to ensure that the devices' latest official updates have been installed and the manufacturer supports the operating system version. A citizen is able to choose and demand more secure digital products. This is also guided by EU level regulation. For example, one objective of the EU's Cyber Resilience Act is to create conditions allowing users to take cybersecurity into account when selecting and using products with digital elements.

Is able to protect used information and look after their digital identity

Is able to protect used information based on its sensitiveness. Masters the basics of protecting digital identity, recognises the importance of protecting against topical threats and knows what measures to take (for example additional certificates in access control). Understands the creation of digital footprint related to identity and the principles of harmful exposure and visibility.

Is able to maintain sense of security and awareness concerning themselves and others

Recognises models of harmful behaviour and their effects in cyberspace. Recognises characteristics of digital violence, violent acts (for example cybercrime and bullying aimed at individuals) and structural violence (for example inequality and possible escalation in digital environment) and knows what to do in these situations. Is able to protect themselves and others against the threats and dangers of digital environment (for example warn others of observed scam attempts). Actively gathers information on cybersecurity and shares it with others.

5.2.1.5. Problem-solving

Is able to solve problems related to the use of services and devices and communicate about problem situations in an understandable manner.

Understands the main principles of the used technologies and knows how to solve the most common problems related to their use. Knows how to seek help in a challenging situation, especially if information security or data protection problems are suspected.

Understands and actively seeks to develop their own competence

Is aware of gaps in their competence or insecurities in using technologies or services. Is determined to develop themselves and understands how their biases, original beliefs and emotional reactions may influence their behaviour in problem situations.

Knows what to do if they become a victim of an information security offence or crime

If an information security offence or crime is suspected, knows how to act to promote both personal and societal security. Understands how their own activities influence incident management, starting from observations. Is able to remain positive when facing and communicating about different problems

References

[954] David Mussington, *Concepts for enhancing critical infrastructure protection: relating Y2K to CIP research and development* (Santa Monica: RAND Corporation, 2002), 30.
[955] Security Committee, "Social Security: Security Strategy for Society", *Government Resolution of 2 November 2017* (Helsinki: Secretary of the Security Committee, 2017).
[956] Mika Helenius, "Human Cyber Security Dimensions - Cognitive Matrix," 21 December 2022, online presentation at an Aalto University workshop.
[957] Riina Vuorikari, Stefano Kluzer and Yves Punie, *DigComp 2.2: The Digital Competence Framework for Citizens*, EUR 31006 EN (Luxembourg: Publications Office of the European Union, 2022).

6. Conclusions

I. The country reports of EU Member States prepared in this study show that their education policies on strategic cybersecurity are quite recent. EU countries are just beginning to create a cybersecurity culture, and the development of digital world is in itself a quite recent phenomenon when compared to the creation of traffic safety culture, for example. Creating and strengthening a culture takes time, calling for a determined effort. That is why measures like the Cyber Citizen project are required right now. Over time, common understanding and extensive competence turn into civilisation and culture that have great importance for the security of the entire society and the security in citizens' everyday life. We must build this kind of civilisation and civic culture to safeguard our security, this time in digital space, and their importance will grow with the advancement of digitalisation and technology.

II. Instead of assigning the responsibility for cybersecurity and its management (technical means) to professionals, EU countries are moving towards integrating cybersecurity into other social activities and making it an integral part of digital world. In practice, this means that digitalisation and digital security are integrated into nearly all human, organisational and social activities instead of being a separate issue. This emphasises the role of cyber citizen skills and their status as one of the basic factors for a functional and sovereign European Union.

III. The threat imaginary in cyberspace has become more diverse and manifold and will keep doing so at an accelerating speed. The rapid changes of the environment, along with the related possibilities and threats, is one characteristic that unites EU countries' understanding of cybersecurity. The EU and the Member States are gaining a better understanding of the complexity of cyberspace. This places a strong emphasis on the importance of continuous development of cyber citizen skills and the scope of developing know-how. Cyber citizen skills should be considered skills that evolve with the changing environment, highlighting the importance of continuous learning in addition to alertness.

IV. Member States have different perceptions of which knowledge and skills are considered cyber citizen skills. Some countries do not have a clear definition of what cyber citizen skills mean in today's society and what knowledge and skills the concept includes. It should also be noted that the definitions vary a lot in the countries that have an official definition. The biggest difference is how technological and/or informative environment cyberspace is considered to be. It can also be noted that the definitions often mean the same but national and cultural differences lead to different ways of expressing it.

V. There is great variation in the basic cybersecurity skills of different EU Member States, and the same applies to the general level of cybersecurity. This can also be seen in the great disparity between countries in the indexes that measure cybersecurity. In addition, countries have different views on how cybersecurity competence and culture should be developed. During the last decade, all countries have created a cybersecurity strategy. However, these strategies mainly provide a national perspective to cybersecurity, not an EU perspective. There is a clear need for developing common cybersecurity culture in the EU, and harmonisation of cyber citizen skills could be an excellent and a big step forward, especially in terms of strengthening everyday cybersecurity in the EU.

VI. There are limited studies on cyber citizen skills in the Member States. In addition, existing studies concentrate on the digital and cybersecurity awareness and behaviour of individuals. Previous studies contain very little information about what cyber citizen skills are learned and taught, how they are taught and how they should be taught. The study on cyber citizen skills in general is very new and has increased in the last few years. Definition of cybersecurity competence citizens have or are expected to have is diverse. It is only now forming and at the moment, it emphasises the concept of digital citizenship. For example, a decade ago the emphasis was on residents and users.

VII. Cyber citizen skills are not considered to include only everyday skills and preparing for threats, but to be an enabler in the ever more digital world (everyday skills and expertise). Instead of a strong emphasis on threats, teaching of cyber citizen skills must focus on the enabling aspect, i.e. that learning cyber citizen skills is an enabler for individuals, organisations and societies. Cyber citizen skills must also be seen as a competitive requirement for the EU in the global technology battle, making the development of cyber competence critical.

VIII. There serious differences between the Member States in how the responsibility for training and teaching cyber citizen skills is shared and assigned. This has a direct effect on the availability of cybersecurity training material and how well it reaches the citizens. Some countries have clearly defined the bodies that produce cybersecurity training material and how to ensure the widest possible dissemination of this material. In some countries, teaching of cyber citizen skills is not coordinated. Teaching is provided by individual bodies and organisations, meaning that they have a reduced impact compared to coordinated teaching at a larger scale.

IX. Because cyber citizen skills apply to us all, the most important things to consider are the psychological and motor differences between various age groups and individuals. This applies to both knowledge and skills and their teaching methods which vary between different groups. There is great divergence between the EU countries in considering the cybersecurity skills of different groups. Differences can also be found in the availability of devices, emphasis on language issues and taking immigrants into consideration. The availability of teaching is essential for the creation of a uniform cybersecurity culture in the EU through competence.

X. In the EU, the selection of available training material is very diverse and dispersed. This applies to both the quality and content of the materials. There are also differences between countries as to what extent cybersecurity skills are included in the curriculum. All in all, this demonstrates that the European Union needs shared definition, teaching and coordination of the teaching of cyber citizen skills. A common foundation facilitates a more common approach between different countries and EU citizens.

XI. The study clearly showed that more trainers of cyber citizen skills are required all over the EU, including trainers who can provide continuing education for teachers in the primary, lower secondary and upper secondary schools. Preparation at EU level and the Member States often place too little emphasis on practical technological skills, and the predictive and multidisciplinary engineering competence related to strategic cybersecurity does not get the attention it deserves in science, research or education policy. The lack of teachers' professional skills in cybersecurity is a clear bottleneck for both teaching general cybersecurity skills and specialisation. Continuing development of these skills is also important due to the ever changing cyber world.

XII. Creating a model based on the current state of cyber citizen competence would be a clear and an important step forward. This calls for a common EU policy the Member States must commit to. A common model for competence building would promote systematic development of digital sovereignty and security preparedness in all EU countries.

XIII. Regulation is one way of guiding the activity and development of society, in addition to economic and information governance. The understanding and model generated by this project should be used at European Union level for competitiveness and information and regulatory issues insofar as the content of curricula is controlled nationally. Research will make it visible that cyber-citizens' skills are essentially linked to the protection of the fundamental rights of members of society, but also that, if not impossible, it will be difficult to achieve without the participation and skills of the citizens themselves.

XIV. Games have established their status as a form of social behaviour, and now play a bigger role as teaching tools. The content of cybersecurity games focuses on the basic skills, critical thinking and

demonstrating threats in digital space. The games analysed in this study were fairly simple and linear. It would be important to recognise different skills levels to adapt the games to the users. This would offer players a better understanding of their digital competence and a chance to develop their skills based on personal needs, regardless of their skills level.

XV. Based on the feedback received during the study, cyber citizen skills should be improved and common European indicators for measuring the skills would be a good idea. The majority of the current indicators of cyber citizen skills demonstrate the level of digitalisation. They lack more specific sections that look at cyber citizen skills. For example, the indicators do not measure citizens' predictive cybersecurity skills, such as programming competence. They also do not consider strategic sovereignty from the perspective of the European Economic Area's continuity and sustainability.

XVI. This study has attracted wide interest in the Member States, and there appears to be a clear need for research. Based on the feedback from EU countries, there is a strong common ground and interest for building common cyber citizen skills in Europe. Also, the conductors of this study have received plenty of guidance and good recommendations on the educational material Prominence is accorded to the importance of general attitude education, the user-friendliness of education materials and continuing development of the teaching content. To summarise, EU countries have a positive attitude towards developing common cyber citizen skills.