EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY EDUCATION INITIATIVES IN THE EU MEMBER STATES

DECEMBER 2022

ABOUT ENISA

The European Union Agency for Cybersecurity (ENISA) has been working to make Europe cyber secure since 2004. ENISA works with the EU, its member states, the private sector and Europe's citizens to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. Since 2019, it has been drawing up cybersecurity certification schemes. More information about ENISA and its work can be found at www.enisa.europa.eu.

CONTACT

For contacting the authors, please use christina.skouloudi@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

ACKNOWLEDGEMENTS

We would like to acknowledge the following experts who have contributed to the study (in no particular order): Christina Skouloudi (ENISA), Chloe Blondeau (ENISA), Solène Vossot (wavestone), Corentin Decock (wavestone), Francois Prost (wavestone).

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-611-8 doi:10.2824/486119 TP-08-22-341-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Today, the internet is a tool used in many educational activities, which increases the amount of time children are exposed to cyberspace and its risks. Informing young users about the importance of maintaining personal privacy is not enough to keep them vigilant when using the internet. More proactive training is required to teach children to be safe online.

Member States, which are advised to increase their cybersecurity capacity, have made efforts to raise cybersecurity awareness among their population through initiatives targeting different age groups of users. With regard to children in particular, the Safer Internet Centers[1], co-funded by the European Commission, have proven to be the main drivers of the majority of initiatives at the national level and have served as a forum for cooperation and exchange of resources.

In line with the European Cybersecurity Act, Article 10[2], ENISA has the mission to focus its efforts in supporting cybersecurity in all levels of education in the Member States. In this context, ENISA has a mandate to support closer coordination and exchange of best practices among Member States on cybersecurity awareness and education.

Additionally, the EU Digital Education Action Plan[3] identifies two priority areas to prepare the next generations for the challenges posed by the digital: i) Fostering the development of a high-performing digital education ecosystem and ii) Enhancing digital skills and competences for the digital transformation. To address these challenges, ENISA recognises the importance of addressing and reshaping the existing cybersecurity education programmes and the continuous changes in the landscape to align the required cybersecurity knowledge and skills.

Through this project, ENISA wants to develop a comprehensive roadmap, towards the implementation of a collaborative campaign at EU level, for enhancing cybersecurity in education - targeting primary and secondary schools - across the EU and create a common platform to foster good practices and knowledge sharing, in order to collaborate with the European Commission (EC) and Member States in the creation and implementation of the required actions.

This study brings out interesting conclusions regarding the best practices around cybersecurity in education across EU Member States, and with-it priorities for ENISA.

Initiatives are often designed by National Cybersecurity Agencies, which then refer to a ministry responsible for the initiatives, but these initiatives may also be designed by that ministry. This usually has an impact on the funding of the initiatives (provided by the state or by private sponsors).

The most recurrent and common key principles to be followed when developing educational cybersecurity initiatives were the following: undertake a collaborative approach to involve various stakeholders, undertake a pedagogic approach to ensure the participation of students, rely on the pareto principle to maximize efforts, construct yearly plans to ensure continuous improvement, educate the parents instead of creating a chain reaction…

Most of the time, KPIs are deployed to measure the achievement of predefined objectives and targets (such as completion of a task, gathering information through a satisfaction survey, web

[1] Safer Internet Centers: https://digital-strategy.ec.europa.eu/en/policies/safer-internet-centres
[2] Cybersecurity Act, Article 10: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&rid=3
[3] Digital Education Action Plan (2021-2027) of the European Commission

analytics to see how many people have participated in a training course, etc.). However, only a few Member States collect KPIs that measure the actual performance of users in the activities. Measuring the impact of cybersecurity education initiatives on the target audience, and whether and how their educational skills have evolved, is a challenge that Member States are trying to study and improve in this area.

The main challenges faced by Member States are the rigid culture of the ministries responsible for educational cybersecurity initiatives, the decentralized approach of some states, the lack of time and resources (low availability of teachers, staff turnover) and the lack of recognition for stakeholders.

Many respondents shared advice on how to approach the ministries responsible for the initiatives, and advice on how to develop initiatives at national level. They would also like to have visibility on what other Member States are doing in terms of cybersecurity in education, and finally they showed interest in working with ENISA and the other Member States.

The goal of this report is to present an overview of the Member States' best practices when implementing cybersecurity education initiatives - targeting primary and secondary schools - as well as the challenges faced by the interviewed stakeholders when carrying out the activities. The aim is to identify the needs and gaps regarding cybersecurity education and determine how ENISA can provide additional support to the Member States.

1. INTRODUCTION

There is a common feature in modern cyberattacks: in most cases, basic computer hygiene such as keeping software updated, using strong passwords, encrypting sensitive data, and keeping copies in the cloud are sufficient to protect computers from such incidents.

For example, one often-overlooked aspect of the 2017 WannaCry attack is that, even though more than 400,000 computers in over 150 countries were hit, millions were not affected because they had updated their software. For this reason, WannaCry was defined as a "tribute to negligence"[4].

As mentioned in the 2017 High Level Group of Scientific Advisors on Cybersecurity to the European Commission[5], many Europeans still fail to take basic cybersecurity measures: many say they care a lot about their personal data, but then give them away for free on social networks. Data are striking: 90% of the data breaches reported by the 2017 Verizon Data Breach Investigation were the result of phishing. And for those who are successfully phished it is not over, because they can expect it to happen again at least once during the same year. Cybersecurity should therefore become a collective responsibility and cyber awareness and computer hygiene should become an integral part of digital literacy programs. Without awareness-raising campaigns and smart policies, cybersecurity will always be dogged by collective action.

1.1 STUDY OBJECTIVES AND SCOPE

In line with the European Cybersecurity Act, Article 10[6], ENISA has the mission to focus its efforts in supporting cybersecurity in all levels of education in the Member States. In this context, ENISA has a mandate to support closer coordination and exchange of best practices among Member States on cybersecurity awareness and education.

The current initiative is consistent with the existing EU Digital Education Action Plan which sets two priority areas to prepare the next generations to face the challenges raised by the digital: i) Fostering the development of a high-performing digital education ecosystem and ii) Enhancing digital skills and competences for the digital transformation.

There is a need for reshaping the content of the existing cybersecurity education programmes in light of the constant evolution of the landscape in order to align the required knowledge and skills.

Through this project, ENISA wants to develop a comprehensive roadmap for enhancing cybersecurity in education across the EU and create a common platform to foster good practices and knowledge sharing, in order to collaborate with the European Commission (EC) and Member States in the creation and implementation of the required actions.

Through desk research and interviews with key stakeholders, and thus the use of primary and secondary data, this report summarises insights around cybersecurity in education collected from Member States.

[4] James Lewis (2017), Darwin and Ransomware, CSIS
[5] "The two most important ways to defend against security threats", CSO (2019)
[6] More information is available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52017PC0477&rid=3

1.2 METHODOLOGY

The study is based on two initial steps: a desk study on the existing initiatives around cybersecurity in education in all Member States, and then a series of interviews with a sample of 14 countries. The results obtained were consolidated in this report. Below is a list of the interviews that were conducted as part of this study.

Table 1: List of interviews

Item	Interviewee	Member State
1	ACN	Italy
2	Hellenic Safe Internet Center & National Cyber Security Authority (NCSA)	Greece
3	NUKIB	Czech Republic
4	INCIBE	Spain
5	University College Dublin (UCD)	Ireland
6	NCSC	Netherlands
7	Service National de la Jeunesse	Luxembourg
8	eSkills Malta Foundation MITA Directorate for Learning & Assessment Programmes at the Ministry of Education FSWS – Appogg MCAST University of Malta	Malta
9	Talinn University of Technology	Estonia
10	ANSSI	France
11	Government Information Security Office	Slovenia
12	National Cyber Security Centre (NCSC)	Portugal
13	Cyber Security Austria	Austria
14	The Swedish Federation of Young Scientists	Sweden

1.3 DOCUMENT STRUCTURE

In this document, the identified initiatives of Member States in the field of cybersecurity education are presented. Good practices are highlighted from the stakeholder interviews, as well as blocking points and challenges.

2. CONTEXT AND BACKGROUND

This chapter provides background information on the context of educating children on cybersecurity issues.

2.1 THE CYBERSECURITY EDUCATIONAL ROADMAP

Along with the increased use of technology in recent decades, the field of cybersecurity has received more attention due to the greater exposure of citizens to ways in which they can be subjected to data theft and damage. The role of cybersecurity experts in protecting critical information and infrastructure, whilst relevant, remains insufficient to cover all internet users due to the shortage of professionals in the market. The solution, which is to address the cybersecurity knowledge level of citizens, requires reaching out to internet users of all age groups, including the new generation.

Schoolchildren are often considered as early introduced to digital technologies and are a critical group to be addressed to ensure that the next generation is well equipped with the skills to use the online space more safely. According to the Cybersecurity Act[7], respectively article 10, ENISA is mandated to "raise public awareness of cybersecurity risks and provide guidance on good practices for individual users aimed at citizens, organisations and businesses, including cyber-hygiene and cyber-literacy", demonstrated through initiatives such as European Cybersecurity Month, European Cyber Security Challenge, European Cybersecurity Skills Framework, CYBERHEAD – Cybersecurity Higher Education Database. At Member State level, the introduction of the cybersecurity topic in school curriculums and activities alone can help ensure that young users are more exposed to and aware of the cybersecurity field and requirements, potentially leading them to choose this domain professionally and helping address the shortage in the labour market.

2.2 LEGAL FRAMEWORK

The Cybersecurity Act, which conferred ENISA a permanent mandate as an agency of the European Union for cybersecurity, describes the goal of focusing efforts in supporting the Member States in "their efforts to raise cybersecurity awareness and promote cybersecurity awareness" (cf. Article 10 Awareness-raising and education).

According to the 2022-2024 Programming Document[8], ENISA's support should be ensured through complementary actions such as capacity building by increasing the supply of qualified professionals to meet market demand and promoting cybersecurity education. Activity 9, in particular, outlines the intention to organise regular awareness campaigns, provide guidance on best practices and support coordination between Member States on awareness and education. The goal is to promote the cybersecurity topics, education and good practices on the basis of the ENISA stakeholders' strategy.

[7] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013
[8] ENISA Programming Document 2022–2024 available here: https://www.enisa.europa.eu/publications/corporate-documents/enisa-single-programming-document-2022-2024

3. CYBERSECURITY EDUCATION INITIATIVES IN EU MEMBER STATES

The mission of introducing young citizens to cybersecurity fundamentals has been expressed in the national strategies of the Member States, which presented their plans of action focused on improving the security and resilience of governments, companies and citizens through improved national infrastructures and increased awareness. With various activities being carried out to ensure that all target groups of society are involved, the introduction of the best practices to children helps ensure that future generations are more apt to face an increasingly digital society.

The table below illustrates the initiatives in cybersecurity education being carried out in the Member States, where it is observed that governments intend on introducing cybersecurity topics through the educational curriculum or training plans carried out in the school setting. From the initiatives corroborated through the desk research and interviews, majority of the initiatives are carried out at national level and pre-teens and teenagers are the target group regularly pursued due to the increased independent use of digital technologies as well as the optimal time to present a new career path before pursuing higher education. Member States like Italy presented specific regional initiatives that will be carried out in additional regions in the future.

Some Member States (40%[9]) showed that on-governmental organization (NGOs) and institutions already involved in carrying out activities with children and adolescents have developed additional initiatives that present and teach the principles of cybersecurity through more practical or engaging approaches such as events, competitions, online platforms, and games. The promotion of the initiatives is usually carried out online or through traditional media. The teaching materials, developed for parents and/or teachers or directly aimed at the target audience, are often available in the institutional or dedicated and available for free.

The list below solely displays the initiatives found through desk research and conducted interviews, not representing an exhaustive scope of all projects currently being carried out in the Member States.

Table 2: Member States' initiatives in cybersecurity education

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
Austria - Cyber Security Austria	**The Austria Cyber Security Challenge** • Type: Talent search initiative • Objective: Identify young talent and present students with a new career path • Scope: Austria • Target audience: 14- to 25-year-old students • Activities: Participate in ethical hacking challenge	Ongoing, with new initiatives to be carried out in 2023, following the organisation of the 2022 European Cybersecurity Challenge in Vienna (to be specified)

[9] Based on the interviews and the desk research conducted, 11 out of 27 Member States have developed initiatives which have more practical and engaging approaches.

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	Cybersecurity training • Type: Training plans • Objective: Teach children and adolescents how to be safe online through games • Scope: Austria • Target audience: Students in primary and secondary school • Activities: Provide trainings about various cybersecurity topics in schools or online • Organised in collaboration with the Vienna Cybersecurity and Privacy Research Cluster, the Learners programme, the Austrian Computer Society, SaferInternet.at and Teach for Austria. **Educational Exchange Platform and the Android and iOS mobile application** • Type: Platforms and applications • Objective: Teach children how to be safe online through games • Scope: Austria • Target audience: Children and adolescents • Activities: Online games and challenges **Support material**: Digital Course Platform from the Ministry of Education, Science and Research.	
Belgium - Centre for Cyber Security Belgium	**Belgian Better Internet Consortium (B-Bico)** • Type: Awareness raising campaigns • Objective: Engage the main Belgian awareness-raising initiatives on cybersecurity, online safety and media education and promote their mutual coordination and outreach, through more dialogue and cooperation • Scope: Belgium • Target audience: Children and adolescents • Activities: Trainings and campaigns **Support material:** Teaching material and campaigns (and the year each project was carried out).	N/A
Bulgaria - Ministry of eGovernment	**Cybersecurity for children and parents** • Type: Online seminar • Objective: Discuss the recent statistics on access of children to the internet and how to educate young users about online safety. • Scope: Bulgaria • Target audience: Parents and teachers • Activities: N/A **Support material:** Recording of the online webinar "Cyber safety for children and parents", organised on 28 October 2021 and with guest speakers from the Parents Association, Applied Research and Communications Fund, Bulgarian Safe Internet Centre and specialists from the Bulgarian Cyber Security Academy.	N/A

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	Bulgarian Safer Internet Centre • Type: Trainings • Objective: Protect and empower children and teenagers by increasing digital literacy and promoting positive, safe and responsible use of the internet. • Scope: Bulgaria • Target audience: Primary and secondary school students, teachers and parents. • Activities: Trainings and campaigns **Support material:** List of trainings provided to students, teachers and parents.	
Croatia - Ministry of Interior	**National Cybersecurity Strategy**: 6.4 - Education, research, development and raising security awareness in cyberspace (I) • Type: Inclusion of cybersecurity within the formal school curricula • Objective: Ensure that students acquire knowledge, skills and competences to successfully ensure their own safe use of information and communication technologies at all levels of formal education, and awareness of the need to protect personal data. • Scope: Croatia • Target audience: Primary and secondary school students, and various population segments • Activities: N/A	N/A
Republic of Cyprus - CYberSafety	**European CyberSafety Projects** • Type: Training and education resources platform • Objective: Bring together the main national stakeholders with the aim of creating a safe internet culture, empowering creative, innovative, and critical thinking citizens in the digital society. • Scope: Cyprus • Target audience: Children • Activities: Awareness and promotional material, helpline. **Support material**: Promotional material	N/A
Czech Republic - NUKIB	**National Educational Plan for Cybersecurity Education and Educational programme framework** • Type: National programmes • Objective: Increase competencies of children and young people • Scope: Czech Republic • Target audience: Primary and secondary school students • Activities: N/A **Educational e-learning portal:** • Type: Platform	N/A

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	• Objective: Develop and maintain an educational e-learning platform to provide the public with cybersecurity awareness on-line courses, campaigns and webinars • Scope: Czech republic • Target audience: Public administration officers, teaching staff, IT administrators, cybersecurity managers, • and other professionals performing ACS-affected roles, as well as vulnerable population groups such as children, young people, and seniors • Activities: Courses, campaigns, webinars **Festival of Safe Internet (FBI):** • Type: Series of educational events, campaigns, conferences and webinars • Objective: Provide visitors with information and advice in the field of cyber security that can be applied to the personal and professional lives of attendees • Scope: Czech Republic • Target audience: Health workers, officials, teachers of primary and secondary schools, teenagers, librarians, senior citizens • Activities: Comic book campaigns for teenagers **Support material**: - Information leaflets - Social media (Facebook and Instagram chat boxes) - Screens in schools, with the cooperation of Amos Vision	
Denmark - Agency for Digital Government	**The Danish National Strategy for Cyber and Information Security** • Type: Curricula and training plans • Objective: Increase competencies of children and young people • Scope: Denmark • Target audience: Primary and secondary school students • Activities: Training courses	N/A
Estonia - Tallinn University of Technology	**Development of curriculum for 1st to 12th grade and extra curriculum activities** • Type: Curricula and training plans • Objective: Support other actors in the country to become better in cyber security. • Scope: Estonia • Target audience: Teachers and students • Activities: Competitions and trainings. **Support material**: - Exercise portal - Competition All materials are made in Estonian, and some are provided in Russian.	Ongoing, with the aim to cover a wider range of schools.

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
European Union – Learning Corner	**Development of a web platform** to share material to primary and secondary schools' pupils and teachers: • Type: Website • Objective: Deploy learning material for kids, on many topics, including cybersecurity. • Scope: EU • Target audience: Teachers and students • Activities: Games, learning material, and teaching material. **Support material**: - Games - Competitions - Activity books - Teaching material	Deployed
Finland - Aalto University	**Development of an educational package on cybersecurity** (open website) • Type: Website • Objective: Teach cybersecurity skills to citizens • Scope: EU (Finland has been awarded EUR 5 million from the EU recovery instrument. The aim will be to share it with all EU countries) • Target audience: All citizens • Activities: Online training courses **Support material**: Exercise portal.	Ongoing, and the aim is to launch the initiative before 2025.
France - ANSSI	**CyberEnJeux:** • Type: Training plan • Objective: Teach the basics of cybersecurity through the creation of a game • Scope: France • Target audience: Secondary school students and higher education (BTS/IUT). • Activities: Provision of a kit with practical information and thematic sheets to guide teachers when creating the cyber game with students **Joint ANSSI – Ministry of Education roadmap on cybersecurity training for students:** • Type: Training plan • Objective: identifying curricula where a cybersecurity dimension could be implemented; training teachers (since then, a mapping has been established of courses and related skills evaluation schemes allowing to integrate cybersecurity); developing cybersecurity educational material (since then: 14 introduction factsheets have been designed); developing innovative training material (since then: CyberEnJeux has been tested in 10 schools with more than 300 students and a release candidate is being now developed). • Scope: France • Target audience: Secondary school students.	Ongoing. All these activities are incubated by ANSSI's innovation Lab in partnership with ANSSI's Cybersecurity Training Center and the Ministry of Education and 110bis, its innovation Lab.

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	• Activities: Introduce the field of cybersecurity through cyber trainings. **Support material** - Kit to develop the game - Pedagogic sheets - Public website **PIX** **SecNumAcadémie - ANSSI:** • Type: MOOC • Objective: Teach the basics of cybersecurity • Scope: France • Target audience: Teenagers and adults • Activities: Cybersecurity MOOC **Association de protection de l'enfance sur internet | e-Enfance:** • Type: Interventions in schools • Objective: Protect children and teens from the dangers of the Internet, fight against cyberbullying. • Scope: France • Target audience: Primary school students to young adults • Activities: Interventions in schools and training on the responsible use of the Internet and possible risks such as cyber-bullying, cyber-sexism and other forms of cyber-violence.	
Germany - Federal Office for Information Security (BSI)	**Guidelines for the federal states** • Type: Policy • Objective: To present guidelines and directions to the federal states, responsible for designing and implementing their own initiatives • Scope: Germany • Target audience: Defined by the federal states • Activities: N/A	N/A
Greece - National Cyber Security Authority (NCSA)	**Promotion of cybersecurity as a profession and gender diversity** • Type: Training plan • Objective: Promote cybersecurity profession to address the shortage of qualified people in the area and the gender gap. The initiative of promoting cybersecurity is owned by the NCSA and carried out with the support of the Hellenic Safe Internet Center and certain Universities. • Scope: Greece • Target audience: Mostly secondary school students and teachers, with some initiatives targeting university students • Activities: Presential and online courses. **Support material** - Talks and webinars - Courses and videos, posters, sharing platform	Ongoing, aiming at intensifying existing partnerships and executing relevant actions plans.
Hungary – National Cyber Security Center	**Hungarian National Cybersecurity Strategy** • Type: Curricula and training	N/A

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	• Objective: Increase competencies of children and young people • Scope: Hungary • Target audience: Primary, secondary, and higher education students • Activities: Training courses **Safer Internet Hungary:** • Type: Awareness raising through educational events, campaigns, conferences and webinars • Objective: Provide children, parents and teachers with information and advice on safe use of the internet • Scope: Hungary • Target audience: teachers, parents and children • Activities: Videos and books **Support material** - Lectures and videos - Games - Events and conferences - Hotline and helpline	
Ireland - University College Dublin	**Cyberwise** • Type: Curricula • Objective: Provide an introductory course on cybersecurity through the Junior Cycle Short Course • Scope: Ireland • Target audience: Primary and secondary school students. • Activities: Courses and competitions **Support material** - Web platform, with short courses - Industry based initiatives (e.g., bootcamps, capture the flags and cybersecurity schools' challenges)	Ongoing, with the aim to expand the initiatives to more schools and get more funding.
Italy - National Cybersecurity Agency (ACN)	Education programmes aimed at primary and secondary schools, universities, and post-graduate training. Specifically: **WeGil ACL Lazio Cybersecurity Academy** • Type: Curricula • Objective: Provide trainings through open to collaboration with universities, high schools, and large Italian information technology companies • Scope: Lazio • Target audience: Upper secondary schools and professionals seeking specialisation • Activities: Courses **Support material:** - Website - Trainings Italy's National Cybersecurity Strategy 2022-2026 • Type: Curricula and training • Objective: Provide cybersecurity education at all levels of education	Cybersecurity Academy is ongoing in the Lazio region, with the aim of extending the initiatives to other regions.

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	• Scope: Italy • Target audience: Students on all levels of education and teachers • Activities: Training and courses National coordination network of Higher Technological Institutes (ITS Academy) for the digital transition • Type: Training • Objective: Promote the development of a national ecosystem for training of new digital skills, support the enhancement of the best experiences, also in the Cloud Computing and Cyber Security fields of the Higher Technological Institutes (ITS Academy), support the training of highly skilled technologists, with outlets at all levels, either in the Public Administration and in the private sector • Scope: Italy • Target audience: Students of Higher Technological Institutes • Activities: Training and courses CyberChallenge.it • Type: Talent search initiative • Objective: Identify young talents in schools and academia • Scope: Italy • Target audience: High school and university students • Activities: Participation in Catch The Flag events and training, and participation in the European Cybersecurity Challenge	
Latvia – CERT.LV (Ministry of Defence) and Ministry of Education and Science	**Latvian Cybersecurity Strategy 2014-2018 and 2019-2022 Strategy** • Type: Curricula and training • Objective: Ensure that society acquires IT skills and master basic online security in order to learn more complex cybersecurity concepts • Scope: Latvia • Target audience: All levels of education • Activities: Training, courses, games and competitions	N/A
Lithuania – Ministry of National Defence	**National Cyber Security Strategy of Lithuania** • Type: Curricula and training • Objective: Provide children and pupils fundamental knowledge of cybersecurity • Scope: Lithuania • Target audience: Students on all levels of education and teachers • Activities: Training and courses	N/A

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
Luxembourg - Service National de la Jeunesse	**BEE SECURE** • Type: Curricula and trainings, campaigns • Objective: Promote a safer, responsible and positive use of information technologies • Scope: Luxembourg • Target audience: Children, adolescents, parents, teachers and the senior population • Activities: Presential trainings, publication of material and events **Support material** - Publications - Interactive tools (Super User, SpamBee)	Maintain all ongoing activities and continuously assess and address future needs and demands.
Malta - eSkills Malta Foundation, BeSmartOnline! and Malta Information Technology Agency (MITA)	**Digital Skills Bootcamp** • Type: Training sessions • Objective: Introduce children to coding and develop the digital skills of individuals. The bootcamp is carried out annually and usually includes cybersecurity courses • Scope: Malta • Target audience: Children and adults • Activities: Training courses Presential events (e.g., Safer Internet Day) • Type: Education and awareness events • Objective: Promote the safe and responsible use of digital technologies • Scope: Malta • Target audience: Students and parents • Activities: School interventions, seminars, theatre plays **Support material** -Social media -Online campaigns -Media outlets -Webinars -Videos	eSkills Malta Foundation will carry out a Cybersecurity Roadshow in collaboration with a private security company. MITA intends on launching a new initiative as part of the national cyber security awareness and education campaign, which will include foundational and advances courses for SOC analysts.
Netherlands - NCSC	**National Cybersecurity Agenda** • Type: Curricula and training • Objective: Revise the existing curricula for primary and secondary education to cover developments in the area of cybersecurity • Scope: Lithuania • Target audience: Primary and secondary school students, teachers, and parents. • Activities: Training and courses **Hackchallenges.NL** • Type: Platform • Objective: Introduce the fundamentals of cybersecurity through cybersecurity games and challenges. • Scope: Netherlands • Target audience: Primary and secondary school students • Activities: Fox book, a website that teaches kids the importance of creating safe passwords, and Catch The Flag, which introduces teenagers to topics such as	Ongoing. The developer of Hackchallenges.NL aims to develop serious games to teach cybersecurity and improve the integration with the Dutch Platform HackShield.

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	hacking, forensics, coding and crypto through challenges. **Support material** -Website	
Poland – National Educational Network	**E-learning portal** • Type: Platform • Objective: Introduce the topic of cybersecurity, as well as other topics such as artificial intelligence, algorithms and programming, databases, biology, chemistry, physics and multimedia. • Scope: Poland • Target audience: Primary and secondary school students and teachers. • Activities: Training courses and competitions. **Support material** -Videos -Publications	N/A
Portugal - National Cyber Security Centre (NCSC)	**National Strategy for Cyberspace Security** • Type: Curricula and training • Objective: Prevention, education and awareness-raising in the cyber field. • Scope: Portugal • Target audience: Primary, secondary, and higher education students • Activities: Actions by the various ministries, with activities dedicated to raising awareness among students, for example. C-LAB • Type: Training platform • Objective: Support citizens, schools and entities by providing a singular platform with trainings based on emerging technologies • Scope: Portugal • Target audience: Students between the ages of 6 and 18 • Activities: Training scenarios **Support material** -Website **Online courses (MOOCs)** • Type: Trainings • Objective: Provide cyber-hygiene skills to citizens by presenting topics such as threats in the cyberspace, how to safely use technologies, misinformation and online shopping • Scope: Portugal • Target audience: All citizens above the age of 14. • Activities: Four different MOOCs (1 - Cybersafe Citizen; 2- Cyber-informed Citizen; 3- Cybersafe Consumer; 4 - Cybersocial Citizen) **CybersecurityChallenge.pt** • Type: Talent search initiative	The action plan of the National Strategy for Cyberspace Security is reviewed annually by the National Cybersecurity Center, where new activities are registered every year (biannual frequency). The action plan is then sent to the High Council for Cyberspace Security (depending on the Prime Minister) where it is approved and ratified. Execution reports are sent to parliament for ratification and political action. Some initiatives are being launched in cooperation with the Portuguese Order of Psychologists. Other activities in preparation include: national campaigns for the cybersecurity month, Safer Internet Day in February 2023, gender parity campaigns and rolling out of activities with the National Association of Teachers of Informatics (ANPRI).

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	• Objective: Identify young talents in schools and academia • Scope: Portugal • Target audience: High school and university students • Activities: Participation in Capture The Flag events and training, and participation in the European Cybersecurity Challenge. **Support material** -Website -Promotional campaigns -Online trainings **Centro Internet Segura & presential events** • Type: Awareness events and sessions, resources, and social media campaigns • Objective: Promote a safer, responsible, and positive use of digital technologies • Scope: Portugal • Target audience: Children, adolescents, parents, teachers, and the senior population • Activities: Presential/ online sessions, seminars, events, and publications. **Support material** -Social media -Website -Online campaigns -Publications / resources	
Romania – Romanian National Cyber Security Directorate (DNSC)	**Cyber Security Strategy of Romania** • Type: Curricula and training • Objective: Promote and consolidate the security culture in the cyber field. • Scope: Romania • Target audience: Primary, secondary, and higher education students • Activities: Educational programs	N/A
Slovakia – National Security Authority	**National Cybersecurity Strategy 2021-2025 of the Slovak Republic** • Type: Curricula and training • Objective: Provide basic security education at all levels of education • Scope: Slovakia • Target audience: Primary school • Activities: Vocational higher and secondary education systems and activities supporting security awareness	N/A
Slovenia - Slovenian Government Information Security Office (URSIV)	Kibertalent.si (Cybertalent) • Type: Talent search initiative • Objective: Spot and attract potential talents for future cybersecurity careers • Scope: Slovenia • Target audience: Students between the ages of 16 and 25. • Activities: Bootcamp and mentoring by cybersecurity experts, and participation in the European Cybersecurity Challenge	The URSIV plans to collaborate with selected secondary schools and faculties to provide cybersecurity workshops locally, and connect academia, industry and R&D institutions to attract more young people to cybersecurity careers.

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	Educational programmes • Type: Curricula and training • Objective: Stimulate the demand for advanced cybersecurity education and increase the supply of cybersecurity educational programmes • Scope: Slovenia • Target audience: Undergraduate and postgraduate students. Later on, to be introduced into the curricula in primary and secondary education • Activities: Educational programs **Support material** -Website -Social media	
Spain - Spanish National Cybersecurity Institute (INCIBE)	**Internet Segura for Kids (IS4K)** • Type: Awareness raising and training • Objective: Provide a helpline service and foster the safe and responsible use of the internet and new technologies. • Scope: Spain • Target audience: Children and teenagers, as well as families, educators and professionals who work with minors • Activities: School interventions and sessions, events, Cyberolympics. **Talent identification** • Type: Talent search initiative • Objective: Attract more professionals to the cybersecurity ecosystem in Spain • Scope: Spain • Target audience: Students over fourteen years old • Activities: Practical labs showcasing how penetration testing and forensic analysis is done, and competitions **Support material** -Website -Social media -MOOCs and training courses -Publications (guides) -Videos -Online workshops -Didactic units	INCIBE is working on developing additional online courses, mainly for families and in collaboration with the internet provider Orange. A course developed in collaboration with the Ministry of Education for educators will be launched in late 2022.
Sweden - Swedish Federation of Young Scientists and Swedish Internet Foundation	**Are you sure? #290CyberSecurity** • Type: Awareness raising • Objective: Show students how to create safe habits online • Scope: Sweden • Target audience: Primary and secondary school students • Activities: Lectures from IT experts **Support material** -Teaching materials - Webpage for the Cybersecurity Academy - Social media posts (Facebook, Instagram, LinkedIn, etc.)	The initiative is ongoing, but the Swedish Federation of Young Scientists is planning to operate the initiative in the long term. It is also planned to develop teaching materials and lectures for grades 1-3 to cover all grades (1-12) and to develop teacher training via online courses in

Country /Entity	Initiative (type, objective, scope, target audience, activities…)	Status and next steps
	- Mailing lists and newsletters	2022 and 2023, as well as face-to-face training. In the long term, the Cybersecurity Academy would like to see the teaching material become standard in all schools, so that every Swedish pupil can learn about cybersecurity systematically.

4. BEST PRACTICES AND MAIN CHALLENGES

This chapter presents the identified best practices in Europe in terms of cybersecurity in education for primary and secondary levels in Europe, based on the interviews.

4.1 GOVERNANCE AND PRIORITISATION PROCESS

This section presents the governance in place in some Member States in terms of cybersecurity in education, as well as the prioritisation process of the educational activities in place.

Governance has been defined to refer to structures and processes (e.g., organisations involved, reporting process) that are designed to build the initiatives. We found various different practices regarding the governance in place in each country. Reporting is defined as the process of regular provision of information to decision-makers – often ministries – within a country to support them in their work. Prioritisation is defined as the specific process of deciding which initiative should be developed and when.

Regarding the responsibility for initiatives, two main practices were observed in the Member State consulted. On one hand (60%[10]), the National Cybersecurity Agencies manage all initiatives (a ministry is always accountable, but the initiatives are designed by the Agency). On the other hand, a ministry itself is responsible for designing the initiatives. The main difference lies in the funding of the initiatives. In the case of the first practice, the Agency has to convince the ministry it refers to "release" the necessary budget and implement the initiatives. In the case of the second, there is no need to find sponsorship. We also saw many different stakeholders involved in the initiatives (i.e., universities, IT companies, other experts…).
These practices are presented in more detail in the following tables:

Table 3: Best practices of Member States regarding governance and prioritisation process

Good practice		Example from a Member State
Organisation, reporting and prioritisation process		
1	The National Cybersecurity Agency is responsible for the initiatives around cybersecurity in education and reports to a ministry in charge.	**ANSSI (France)** and the Ministry of Education work together towards developing cybersecurity training and education, but there are no strong sponsorships for the activities. The topic of cybersecurity training and education for the youth is identified as a political priority but remains an emerging challenge to be tackled in years to come in France. **NUKIB (Czech Republic)** ´s director reports directly to the prime minister. NUKIB cooperates its activities with the Ministry of Education, Youth and Sports as an equal partner. The ministry is responsible for overall education strategy and NÚKIB is the coordinator of cybersecurity educational activities (it makes sure that cybersecurity education aspects are considered and included). **INCIBE (Spain)** reports to the Ministry of Economic Affairs and Digital Transformation.

[10] Based on the interviews conducted with 16 Member States, 9 out of 16 Member States indicated that the National Cybersecurity Agency designs and takes the lead for all initiatives.

	Good practice	Example from a Member State
2	A Ministry (or multiple ministries) is responsible for the initiatives and plays a role of sponsor. It gives the go-ahead to the National Agency.	In **Luxembourg**, the Service national de la jeunesse (SNJ) is the coordinator of the governmental initiative BEE SECURE, and the SNJ is attached to the Ministry of National Education, Children and Youth; Three ministries support the initiative (the Ministry of National Education, Children and Youth, the Ministry of economy, the Ministry of Family Affairs, Integration and the Greater Region).
3	A community of experts is involved in the initiatives.	In **Italy**, ACN has set up a working group of stakeholders from universities, high schools, and IT companies. In **Malta**, MCAST Hackspace, sponsored by eSkills Malta Foundation and supported by MITA, Cybersecurity Malta and Industry. Hackspace is a virtual and physical space where students take part in security dialogues between themselves and with Industry partners and also include cybersecurity sessions for further learning. In **Estonia**, a board of experts lead the initiatives with the help of a community of teachers. In **Ireland**, UCD works with other schools, and a lot of non-for-profit organisations. This is facilitated by a working group of cybersecurity education stakeholders, organised by the Ministry for Communications, which oversees the National Cyber Security Centre.

We also identified two different practices regarding funding. Funding is the means by which the money required to undertake an initiative is secured and then made available as required. Both practices depend very much on the reporting presented above. In the first practice, which usually occurs when initiatives are launched by a ministry, funding is provided entirely by the ministry. The second occurs when the ministry responsible does not fund the initiatives.

Table 4: Best practices of Member States regarding funding

	Good practice	Example from a Member State
	Funding	
4	Funding is provided by the state.	In **Ireland**, **UCD** receives fundings form the Public Service Innovation Fund in the Department of the Environment Climate and Communication.
5	Funding is provided by private sponsors (industry) or other means of implementing the initiatives are found.	In **Austria**, the Ministry of Education is not implicated in the initiatives and is not willing to fund those. The **CSA** thus works with a lot of organisations that do not charge for their training and courses.

4.2 MEASUREMENT MECHANISM

This section presents the mechanisms that have been implemented in some Member States to measure and monitor the effectiveness of the initiatives, as well as their completion.
The effectiveness of a project could be defined as the degree to which the objectives are met, within the deadlines, respecting the agreed budget. The effectiveness of a project or initiative can be measured by creating indicators (KPIs) to measure the level of performance.
There are different types of indicators, and it is possible to collect indicators them by different means of data collection, (surveys, metrics (in a website), interviews, etc). After the collection of data, you need to analyse and interpret the data to be able to make decisions based on the results obtained.

Regarding the initiatives, the effectiveness can be considered as the degree to which the students are being educated in cybersecurity.

The KPIs are usually deployed to measure the completion of the objectives: follow up on the daily activities (task completion); collecting feedback form participants and all stakeholders; collection of analytics from websites and apps. Only some Member State actually collect KPIs which measure the performance of the users in the activities. Measuring the impact of initiatives on the target audience is complex.

Table 5: Best practices of Member State regarding measurement mechanism

	Measurement mechanism	Example from a Member State
1	Collection of task completion indicators that reflect on the level of completion of a specific initiative	**NUKIB (Czech Republic)** and ACN (**Italy**) both implemented a KPI for task completion of its national plan.
2	Feedback collection from participants of an initiative (teachers and other stakeholders, students) to measure the implication of stakeholders	**UCD (Ireland)** collects feedback from the participants after each initiative
3	Collection of indicators of number of people using a service to measure visibility and attractiveness of those services	**INCIBE (Spain)** collects indicators on the number of people who have used their services: gender, age, geographical location…
4	Observation of the performance of the users in the activities	**NCSC (Netherlands)** observes if users are able to conclude the objectives or not, and if additional tips should be added
5	Collection of analytics from websites and apps to measure the effectiveness	**SNJ (Luxembourg)** uses analytics from their website, their social media accounts, and the campaigns they conduct

4.3 KEY PRINCIPLES

This section presents the key principles that have been followed in developing the initiatives of the interviewed Member States.

Various key principles were highlighted by the Member States. These principles guided the approach taken by organisations in designing and deploying the initiatives. We found that the key principles were often shared by many Member States.

The table below summarises the key principles that are followed by Member States in implementing and designing their initiatives:

Table 6: Key principles followed by the Member States

	Key principle	Example from a Member State
1	**Collaborative approach**: basing the initiatives on close collaboration with stakeholders (ministries, schools and teachers, industries, and other experts…)	On top of the initiatives presented above with regard to the experts' communities: in **Slovenia**, The URSIV plans to collaborate with selected secondary schools and faculties to provide cybersecurity workshops locally, and connect academia, industry and R&D institutions to attract more young people to cybersecurity careers.
2	**Pedagogic approach**: actively involve students in the activities	In **France**, ANSSI has created a kit designed for kids to allow them to develop a cyber game
3	Pareto principle: looking for multipliers to try to get maximum results by exploiting the least amount of resources	In **Greece**, the NCSA is forming strategic partnerships with esteemed stakeholders, in order to reach wider audiences and benefit from their proven know-how.
4	Preparing **yearly plans** to have a step ahead of the next initiatives	In **Malta**, MITA focuses on preparing and executing yearly plans that address the challenges and trends in the field of cybersecurity, whilst still maintaining a plan flexible enough to tackle new problems
5	Educating children through the **parents**: creating a **chain reaction** which starts with the parents and reaches all levels of education	The eSkills Malta Foundation leads initiatives for parents on how to make wise use of social media and the consequences of misuse (e.g., go to the parent's place of work and provide sessions about online safety), in order for the parents to have the best behaviour and therefore become good examples for their children.

4.4 COLLABORATION WITH OTHER ORGANISATIONS, INCLUDING ENISA

This section presents the existing collaborations between organisations, countries, or ENISA, in the field of cybersecurity education initiatives, in order to streamline activities or learn from each other, share good practices. The collaboration can have different purposes, such as obtaining more budget, or gaining expertise.

In conducting the interviews, we often noted that the interviewees stressed that they would really like (if not already do) to work with ENISA and other Member States. For most Member States this is not yet the case. We have noted only a few of these, which are listed in the table below.

Table 7: Best practices of Member States regarding collaboration

	Collaboration practice	Example from a Member State
1	Collaboration between countries	**Estonia** works on a regular basis with Norway: they organise a cybersecurity education summer camp and a cybersecurity competition together.
2	Collaboration with ENISA (use of ENISA material)	In **Italy**, **ACN** uses the European Cybersecurity Skills Framework -developed by ENISA - for the identification of professional profiles to be trained at the Lazio Cybersecurity Academy.

5. CONCLUSIONS

This chapter presents the main findings of the study, in particular it highlights the main challenges and obstacles faced by EU Member States in implementing cybersecurity initiatives in education within their countries and summarises the key priorities that ENISA should focus on for the EU cybersecurity education roadmap.

5.1 CHALLENGES ENCOUNTERED

This section presents any challenges or barriers encountered by the Member States in implementing the Cybersecurity Education initiatives within their countries. A challenge can be defined as a fact or process which has made (or still makes) the initiatives difficult to deploy, or even prevented the initiative from reaching the expected level.

Below is a list of challenges faced by the Member States encountered in the deployment of the initiatives:

- **Rigidity of anchored culture of the ministries** responsible for the cybersecurity initiatives in education: The culture, which leads to cybersecurity being treated as a secondary topic (as mentioned in the previous section), leads to a slow pace of change management within these public bodies, which prevents national cybersecurity agencies - or any other organisation designing the initiatives - from deploying them at national level.

- **Decentralized approach**: In Germany and Austria, the country is divided into a number of federal states, which have a certain amount of autonomy at many levels, including in terms of educational strategy. This makes it impossible for them to implement national initiatives, and very difficult to monitor local initiatives.

- **Lack of time and resources**:
    - **Teachers' low availability**: In some Member States, initiatives are launched locally with teachers in their free time, which is very limited. It is then very difficult to have them participate due to their low availability.
    - **Staff turnover**: In some Member States, there is a high turnover in the teams working on the initiatives. It is thus difficult to maintain the activities of the initiatives on a long term.

- **Lack of stakeholder recognition**: Stakeholders who participate in initiatives, sometimes in their spare time (e.g., teachers in many Member States), might not receive enough recognition, which could further motivate them to participate in initiatives. For example, it was mentioned that teachers could get a certification or a badge, when they implement an initiative at school and the sense of ownership or confidence, they are given could motivate them further.

- **Need to take into account the different languages spoken in a country**: In Luxembourg, Belgium or Austria, for example, initiatives and especially support materials need to be developed in the different languages of the country in order to reach all the students.

5.2 KEY PRIORITIES FOR THE ENISA ROADMAP

This section presents the key priorities that ENISA should focus on for the EU cybersecurity educational roadmap.

- **Advice on how to approach ministries**: For many Member States, the anchored culture of the ministries responsible for the initiatives relegates cybersecurity, and in particular the cybersecurity education field to the background. This makes it difficult to push initiatives at national level and to get funding. Those Member States believe that ENISA is in a strong position to convince the national authorities of the importance of cybersecurity education, and to give them the keys on how to address the challenges.

- **Advice on how to develop initiatives at national level**: In some Member States, such as Germany and Austria, the autonomy of the federal states within the country makes it difficult to deploy initiatives at national level, and hampers progress on this area. Those Member States hope that ENISA has the capacity to be the backend/coordinator of the topic and identify and encourage local authorities to develop educational initiatives.

- **Visibility on what the other Member States are doing**: Many Member States expressed their willingness to compare and discuss existing initiatives deployed in other Member States. By doing so, the Member States would be able to learn from each other and make the most out of each State's best practices, challenges encountered, and key lessons regarding those initiatives.

- **Encourage Member States to engage in partnerships with the private sector (e.g., industry):** While some Member States already engage in this kind of partnerships (e.g., Italy, Slovenia…), most Member States miss on this opportunity to access more technical / operational point of views, and also to build a multi-disciplinary team. Indeed, this partnership with the private sector would allow to a collaborative approach around decision making process and implementation of cybersecurity innovation initiatives.

TP-08-22-341-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-611-8
doi: 10.2824/486119