EUROPEAN UNION AGENCY
FOR CYBERSECURITY

CYBERSECURITY EDUCATION MATURITY ASSESSMENT

MAY 2024

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.

CONTACT

For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Christina Skouloudi (ENISA), Evangelos Kantas (ENISA)

Solène Drugeot (Wavestone), Débora Lopes Goncalves (Wavestone), Francesco Principe (Wavestone), Solène Vossot (Wavestone)

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) 2019/881.

ENISA has the right to alter, update or remove the publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partially must contain ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources, including external websites, referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN 978-92-9204-674-3, DOI 10.2824/3832

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As described in Article 10 of the Cybersecurity Act (1), ENISA has the mission to focus its efforts in promoting cybersecurity in all levels of education in the EU Member States (MS). In this context, ENISA has a mandate to support **closer coordination and exchange of best practices among MS on cybersecurity awareness and education**, a task that has also been included in the ENISA Cybersecurity Education Roadmap (2).

On one hand, this ENISA study aims at designing and developing a maturity assessment model to assess each MS maturity level regarding cybersecurity education in the **primary and secondary levels** and **obtaining a comprehensive state of play of the EU**. On the other hand, in addition to quantitative scoring reflecting national maturity levels, ENISA's objective was to **collect and disseminate recommendations and good practices among countries**.

Quantitative results obtained from primary and secondary education data (3) collected from 15 and 27 MS respectively show that on average a range of MS in the EU have a level of maturity of 66 %, which corresponds to level 4 out of 5 ('Establishment'). This means that MS already have a series of initiatives in place for cybersecurity education. However, national approaches strongly vary from one country to another and mostly rely on decentralised initiatives or stand at the infancy stage of implementation.

66%

Cybersecurity Education maturity level in the EU ("Establishment")

More specifically, ENISA assessed maturity levels according to three dimensions: 'Governmental' (70 %), 'Strategic' (64 %) and 'Operational' (63 %). One of the main takeaways is that while cybersecurity education initiatives are generally supported by a national regulatory framework, they strongly rely on **national cybersecurity strategies**. In fact, these tools usually provide European stakeholders with guidelines and support to include the cybersecurity topic into school curricula; this significantly fosters the adoption of cybersecurity in the primary and secondary levels of education. The involvement of **government-appointed entities and cooperation with private sector actors** was identified as a major pillar for fostering cybersecurity in education.

Lastly, in this study ENISA lists **best practices and recommendations** addressed to MS per maturity level, available for each dimension of the maturity assessment model, along with concrete examples of country initiatives and contact points of national organisations.

(1) Cybersecurity Act of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) (OJ L 151, 7.6.2019, pp. 15–69, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(2) ENISA, 'Cybersecurity education'. The roadmap is not publicly available.

(3) Primary data refers to information collected via stakeholder consultation when interacting directly with the target respondents (e.g. interviews, workshops, focus groups). Secondary data refers to information collected via desk research and researchers' own investigations (e.g. websites, articles, books).

1. INTRODUCTION

1.1 CONTEXT OF THE STUDY

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, while relevant, remains insufficient to cover all internet users due to the shortage of professionals in the market. The solution, which is to increase 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 being introduced early to digital technologies (also called 'digital natives') and are a critical group to address to ensure that the next generation is well equipped with the skills to safely use the online space. According to Article 10 of the Cybersecurity Act, ENISA is mandated to support closer coordination and exchange of best practices among MS on cybersecurity awareness and education, as shown in the Cybersecurity Education Roadmap and demonstrated through initiatives such as European Cybersecurity Month, the European Cyber Security Challenge, the European Cybersecurity Skills Framework and the Cybersecurity Higher Education Database, known as CYBERHEAD.

At the MS level, the introduction of the cybersecurity topic in school curricula 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 to address the cybersecurity expert shortage in the labour market. Nevertheless, there are still variations across MS in term of cybersecurity education maturity. Consequently, one of the main priorities identified by ENISA in its European Cybersecurity Roadmap was the need to identify the level of maturity of each MS and obtain an EU state of play, along with favouring exchanges of good practices and providing recommendations on different cybersecurity education dimensions covered in the report (e.g. guidelines, educational toolkits, standards and partnerships with stakeholders).

1.2 OBJECTIVES AND SCOPE

As a continuation of the ENISA report *Cybersecurity Education Initiatives in the EU Member States* ([4]), ENISA aims to understand the maturity of cybersecurity in primary and secondary education in each MS to further allow the creation of specific material to support cybersecurity education according to the different maturity levels identified. This project will then lead to the outlining of concrete activities over multiple years, such as the development of educational tool kits, guidelines, standards and stakeholder partnerships. In light of this ultimate goal, ENISA will develop this report on maturity assessment for cybersecurity education. The objectives of this project are to:

- select the maturity model suitable for assessing maturity of cybersecurity education in each MS and support the maturity assessment;
- define relevant maturity levels and assess maturity of cybersecurity educational activities per MS;
- draw recommendations on national initiatives and good practices per dimension of the maturity assessment model and per maturity level.

([4]) ENISA, *Cybersecurity Education initiative in the EU Member States*, December 2022. Available at: https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states.

1.3 DOCUMENT STRUCTURE

Section 2 presents the maturity assessment results across dimensions and countries. This section is illustrated by country use cases including relevant practical applications of good practices. Lastly, Section 3 summarises recommendations per dimension addressed to the MS and presents MS expectations toward ENISA. The methodology selected and applied to the maturity assessment framework and the data collection approach is presented in the Annex of this report, which is distributed as a separate document.

2. MATURITY ASSESSMENT OF EU MEMBER STATES

This section presents the main results of the maturity assessment carried out as part of this study in the field of cybersecurity in primary and secondary education'. **Readers should note that the calculations and graphs presented in this study take into account the contributions of the 15 MS that participated in the data collection**. Unanswered questions were treated as 'Not available', i.e. N/A. In order to present statistically representative quantitative data, countries with more than a third of 'Not applicable' responses were not included in these calculations. The **sample is therefore reduced to 13 countries** (i.e. two consulted countries provided more than a third of their responses as 'Not applicable', so their results were not statistically representative for the quantitative part of the analysis. However, for the qualitative part, more specifically for the overall state of play of the MS and their good practices around cybersecurity in education, their relevant contributions were taken into account).

Three dimensions were specifically developed to reflect the different ways in which cybersecurity in education could be ensured, promoted and implemented within and across the MS, as depicted in Table 1.

Table 1 – Dimensions and sub-dimensions of the maturity model

Dimension	Sub-dimension
1. Governmental	1.1 Regulatory framework
	1.2 Policies
	1.3 Support
2. Strategic	2.1 Strategies
	2.2 Action plan
	2.3 Cooperation
3. Operational	3.1 Provision of education
	3.2 Uptake of education

The following table illustrates the different levels of maturity in terms of cybersecurity education per dimension of the model, along with the average of a range of EU MS. The EU average is calculated by taking into account the maturity levels of the 13 MS in the sample.

Table 2 – Maturity levels

Maturity level	Score in %
1. Non-existent	0–20 %
2. Initial/ad hoc	20–40 %
3. Definition	40–60 %
4. Established	60–80 %
5. Optimised/refined	80–100 %

The methodology selected and employed to the maturity assessment framework and the data collection approach is presented in the Annex of this report, which is distributed as a separate document.

2.1 MATURITY AT THE GOVERNMENTAL LEVEL (DIMENSION 1)

This subsection aims to provide a more detailed assessment of the **governmental dimension** of the maturity model governing the implementation of cybersecurity education. It builds on the insights collected through the detailed desk research on the 27 MS and the detailed insights gathered through the 14 interviews and 3 responses received from the online survey. Liaising with MS representatives enabled ENISA to identify good practices that complemented the findings issued from desk research. These good practices are presented later in this section in Table 6.

As indicated in the previous section, the governmental dimension encompasses all **actions and aspects taken at the political level** with regard to cybersecurity education in primary and secondary education, including regulations and policies defining the regulatory framework (planned or implemented). In order to measure the level of maturity of MS in the field of cybersecurity education, it was essential to analyse their political maturity in this area. The governmental dimension is assessed through **three main sub-dimensions** relating to governmental initiatives at the national level. As presented in the theoretical framework (Table 1), these three sub-dimensions are **Regulatory framework, Policy and Support**.

A majority of the countries indicated that they had implemented or planned to implement a policy to support the adoption of cybersecurity education measures at the national level, translating to a 78 % maturity level. However, MS tend to be less advanced when it comes to having a comprehensive regulatory framework in place to shape policy, as shown by the average maturity level of 64 %. Finally, the countries show a medium maturity level (56 %) in relation to supporting education and/or cybersecurity stakeholders and organisations through national programmes. In fact, less than half of the countries reported having programmes in place involving activities that would be fully or partially funded by national budget schemes.

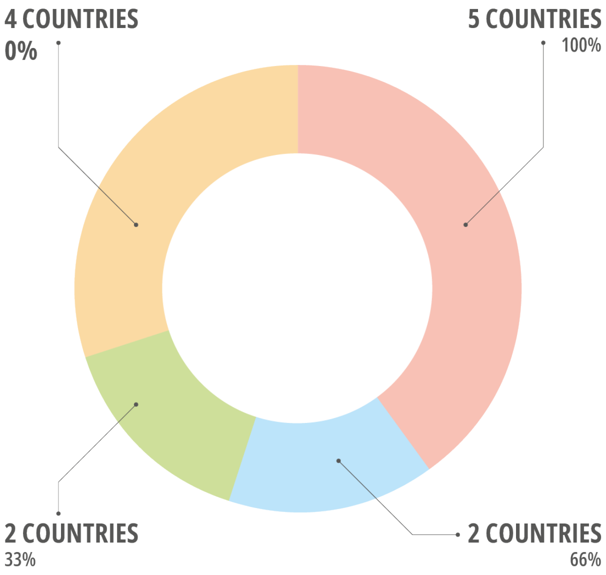
The analysis of each sub-dimension is detailed in the following sections: Assessment of regulatory framework, Section 2.1.1; Assessment of national policies, Section 2.1.2; and Assessment of national support, Section 2.1.3.

2.1.1 Assessment of regulatory framework (sub-dimension 1.1)

Referring to the regulatory framework indicators, Figure 1 shows that 5 MS over the 13 countries represented have implemented a regulatory framework. In most countries, regulatory frameworks tend to be aimed at political decision-makers. However, it was also observed that regulatory frameworks can be aimed at private organisations. Two other countries are in the process of defining a regulatory framework (‘Establishment phase’) to support the development of a multiannual educational programme applicable at the national level. The two remaining countries, with a maturity score of 33 %, tend to be more 'strategic'-oriented and devote fewer resources to policy work. The 33 % means that these countries are either in the development phase of these policy initiatives or are only acting politically on an ad hoc basis. As for the four countries with a maturity score of 0 %, they have no policy initiatives at all.

The findings from the desk research show that all 27 MS rely on national cybersecurity to define actions relating to cybersecurity education. While the emphasis varies greatly from one national strategy to another, these strategies focus on concrete actions and a definition of governance based on national cybersecurity strategies. This will be discussed in more detail in Section 2.2.

Figure 1 – Member States' maturity on the implementation of regulatory framework to support cybersecurity education (by numbers of countries)



Source: Authors' elaboration (data analysis based on the sampled countries, 13 in total).

The idea behind defining a regulatory framework for MS is to define common goals, scope and objectives for ministries of education, ministries responsible for digital and cybersecurity issues, government entities and public and private stakeholders involved in cybersecurity education. However, MS representatives often pointed out that education and cybersecurity are generally seen as two different subjects, dealt with and supported separately. It was also observed that countries with a federal or regional structure manage education in a relatively heterogeneous way. Consequently, the development and implementation of a single national regulatory framework on cybersecurity education is seen as a complex and inadequate task, due to the diversity of stakeholders and organisations involved, and sometimes language barriers.

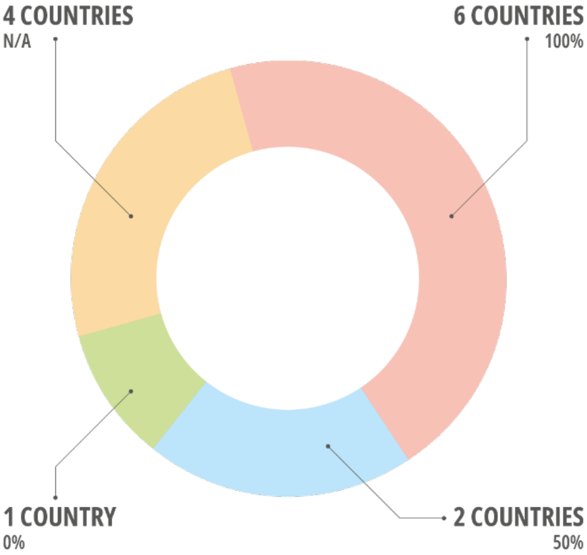
Finally, the mandatory inclusion of cybersecurity education in school curricula is seen as an effective way of ensuring the adoption of these measures in schools. However, geographical and demographic issues similar to those mentioned above apply when it comes to developing a single programme for a country. Currently, 4 of the 27 MS are not considering the implementation of a cybersecurity curriculum.

2.1.2 Assessment of national policies (sub-dimension 1.2)

All the MS consulted stated that they had transposed the NIS Directive ([5]) enacted in 2016. In addition to legal transposition, of the 6 countries that said that they had drawn up national policies, 3 pointed out that the policies tended to target universities rather than the primary and secondary levels or provided no details at all. Lastly, of the two countries with a maturity level of 50 %, one indicated that it acted as a national organisation available to share advice and support the adoption of cybersecurity education; however, national coverage of a policy is compromised due to the nation's regional government structure. Only one country out of 13 indicated that there was no national policy in place or planned.

One should note that 4 countries did not provide data for this indicator. These are shown as N/A in Figure 2.

Figure 2 – Member States' maturity on the implementation of a national policy to support cybersecurity education



Source: Authors' elaboration.

2.1.3 Assessment of national support (sub-dimension 1.3)

As mentioned in Section 2.1, 'national support' refers to the launch of programmes or initiatives that would concretely support MS in setting up measures to promote cybersecurity in education from a regulatory point of view. A total of six countries reported having a national programme in place or planned, including a series of initiatives developed at the governmental level.

One of the best performers has had a national programme in place since 2023, supported by an active working group and aimed at developing digital and ecological skills in all vocational curricula.

Eight other countries have indicated that there is no national programme in place, but rather ad hoc initiatives that are not necessarily part of a structured national programme.

[5] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (OJ L 194, 19.7.2016, pp. 1–30, ELI: http://data.europa.eu/eli/dir/2016/1148/oj).

Figure 3 – Country example of national policy actions conducted at the national level

In France, the NIS Directive (2016) was transposed at the national level. Additionally, the Ministry of Education has set up guidelines relating to cybersecurity education; however, there is no written regulatory framework.

Cybersecurity has been introduced as an official topic of school curricula in France. In primary schools, lessons are focused on digital hygiene/security while in secondary schools, the cybersecurity topic is part of the curricula for students attending the mathematics or IT branches.

For the academic year 2023–2024, the **digital education** subject will be introduced to students in the *6ème* (10–12-year-olds). **Cybersecurity topics** will become mandatory for students in the *3ème* (14–15-year-olds) and in the end of the *lycée* (17–18-year-olds). Students are required pass an exam on these topics. Lastly, there is a specific mandatory curriculum with cybersecurity items for the professional branch called *Baccalauréat professionnel CIEL*.

While there is no specific policy, the Ministry of Education has rolled out over the 2 past years a roadmap to encourage students to pursue a cybersecurity career. It also provides guidance for pupils who want to follow a cybersecurity career and recommendations for teachers to pupils on cybersecurity topics for primary and secondary schools, through the éduscol platform.

The Ministry of Education uses the Pix platform to assess the digital skills of the population. The platform was built in collaboration with ANSSI and Cybermalveillance.gouv.fr. The platform evaluates students' skills based on five domains (the fourth being 'Protection and security'). The test is based on the EU Digital Skills Assessment Tool and helps understand the level of digital skills of French students and adapt their cybersecurity education experience.

2.1.4 Good practices on governmental aspects (Dimension 1)

In addition to concrete governmental initiatives, the objective of the targeted consultation was to collect good practices around cybersecurity education at the governmental level. Table 3 presents a series of good practices illustrated by inspiring national actions.

Table 3 – Good practices identified at the national level (Governmental dimension)

Good practice		Sub-dimension	Case study from a Member State	
1	Develop a national policy or guidelines to guide education stakeholders in their adoption and teaching of cybersecurity topics	National policy	🇮🇪	The National Cyber Security Centre of Ireland has produced guidelines entitled 'Quick Guide: Cyber Security for Schools', https://www.ncsc.gov.ie/pdfs/NCSC_Quick_Guide_Schools.pdf. This guide aims at assisting primary, post-primary and specialised schools in particular to implement the key priority measures that can help to reduce the likelihood of a school becoming a victim of a cyberattack or to reduce its impact.
2	Explicitly include cybersecurity education in primary and secondary school curricula	National policy	🇱🇺	Cybersecurity is mandatory in some secondary school sections. There is a new course called Digital Sciences that includes six modules, one being 'The world wide web, its network and me', which is being developed in collaboration with BEE SECURE.

				In this module, students undergo 2 mandatory hours focused on online safety, which includes cybersecurity. This activity serves mostly as an awareness activity and students are not graded. Secondary level schools in Luxembourg offer different sections: Section I (Informatics), where students follow cybersecurity courses (*sciences cognitives and sciences humaines*) that will be introduced in the 2024–2025 academic year, will address the topic of GDPR (in the second to last year of secondary school, *deuxième*). Schools can book BEE SECURE training sessions for their classes from grade 3 onwards.
3	Support teachers by providing clear guidance on pupils' learning path (i.e. skills / knowledge to be acquired)	Support	🇫🇮	For the support of teaching staff, concrete examples as The Framework for Digital Competence has been created by the Finnish government to describe the learning pathway starting from early childhood education and care: https://eperusteet.opintopolku.fi/#/en/digiosaaminen/8706410/osaamiskokonaisuuspaaalue/8709072.
4	Define clear governance and appoint an entity in charge of supporting teachers	Support	🇪🇸	The Spanish National Cybersecurity Institute is the reference entity to drive a better use of internet for minors in Spain, and it works within the framework of the EU's BIK (Better Internet for Kids) strategy. The institute manages Internet Segura for Kids, the Spanish Safer Internet Centre that takes part in the Insafe and INHOPE networks, and also operates services to promote a safer and better use of the internet and mobile technologies among children and young people: an awareness-raising centre, a helpline, a youth participation initiative, a hotline and the organisation of the Safer Internet Day.

2.2 MATURITY AT THE STRATEGIC LEVEL (DIMENSION 2)

This subsection aims to provide a more detailed assessment of the second dimension of the maturity assessment model, the **strategic dimension** governing the implementation of cybersecurity education. This section will build on the insights collected through the detailed desk research on the 27 MS and the detailed insights gathered through the 13 countries represented, thanks to the data collection activities and result computations within the theoretical framework. Additionally, good practices identified through interviews and/or the detailed desk research will be highlighted in Section 2.2.4.

As per the theoretical framework presented in Section 2.2, the 'strategic' dimension is divided into three sub-dimensions: **Cooperation, National strategies and Action plan**. The EU average shows results from 64 % to 74 % in terms of maturity level across this sub-dimension. This means that the MS position themselves in the 'Establishment' phase of any strategy action fostering the adoption of cybersecurity education measures.

Each sub-dimension is detailed in the section below as follows: Assessment of national educational strategies, Section 2.2.1; Assessment of national action plans, Section 132.2.2; and Assessment of national initiatives to foster cooperation, Section 2.2.3.

2.2.1 Assessment of national educational strategies (sub-dimension 2.1)

National education policy is defined as 'a comprehensive framework for elementary education to higher as well as vocational training'. This aims at supporting quality education, training and social cohesion at the national level [6]. In the context of this study, national education policy informs about the different mandatory/voluntary topics included in curricula for the primary and secondary levels.

As observed in all MS, national cyber security strategies (NCSS) are the tools most frequently used to support the implementation of cybersecurity education initiatives at the national level (for both primary and secondary education, or for secondary education only). In most countries, elements relating to cybersecurity education are fully taken into account in their NCSS (7 countries show an 'Optimised/adapted' level; 100 %). In some of these countries, national strategies indicate that cybersecurity topics and aspects should be covered in primary and secondary schools, and eventually integrated into official national curricula. In 4 other countries, cybersecurity education is briefly mentioned in the NCSS (showing an 'Establishment' level; 66 %). Of the 13 countries in the sample, only 1 does not consider cybersecurity education as part of its national cybersecurity strategy.

Alternatively, or additionally, MS may choose to communicate cybersecurity education in their national education policy (or in an equivalent legal instrument used at the national level to frame educational aspects in the country). Figure 5 shows that, on the one hand, 8 countries have reached a maturity level of 100 % on this aspect. On the other hand, a third (4) of the countries consulted claim not to mention cybersecurity education in their national education policy. In fact, representatives from these countries reported difficulties in cooperating with education ministries at the national level, as they tend to be inflexible and reticent about cybersecurity topics and innovations. It has also been reported that ministries of education may have other priorities for the school system, leaving no room for cybersecurity-related topics as part of the curriculum or additional electives for students. This difficult cooperation therefore presents national organisations with the opportunity and need to adapt and follow a bottom-up approach, taking into account centralised initiatives (e.g. safer internet centres, national cybersecurity centres, working groups, government entities created specifically for cybersecurity education) and/or industry initiatives. As discussed further in the 'Operational dimension; Section 4.3', this tends to result in heterogeneity between schools' initiatives (including between regions of the same country) in cybersecurity education and in unequal access to cybersecurity knowledge between public and private schools.

[6] European Union, 'Education Training and Youth', 2023. Available at: https://european-union.europa.eu/priorities-and-actions/actions-topic/education-training-and-youth_en.

Figure 4 – Member States' maturity on the consideration of cybersecurity education within their national cybersecurity strategy

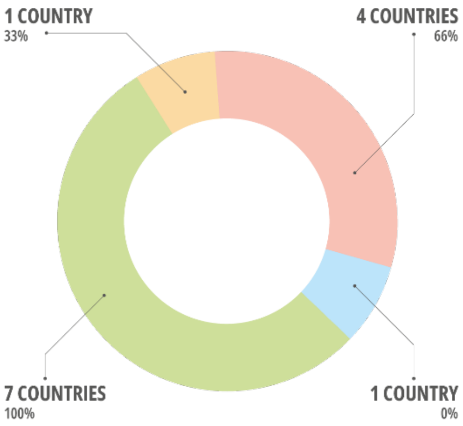
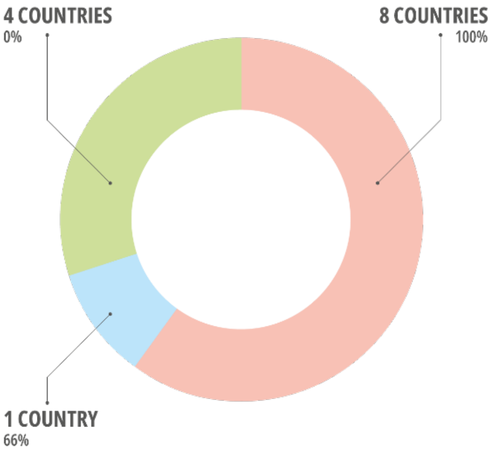


Figure 5 – Member States' maturity on the consideration of cybersecurity within their national education strategy (or equivalent national initiative)



Source: Authors' elaboration (data analysis based on the sampled countries, 13 in total).

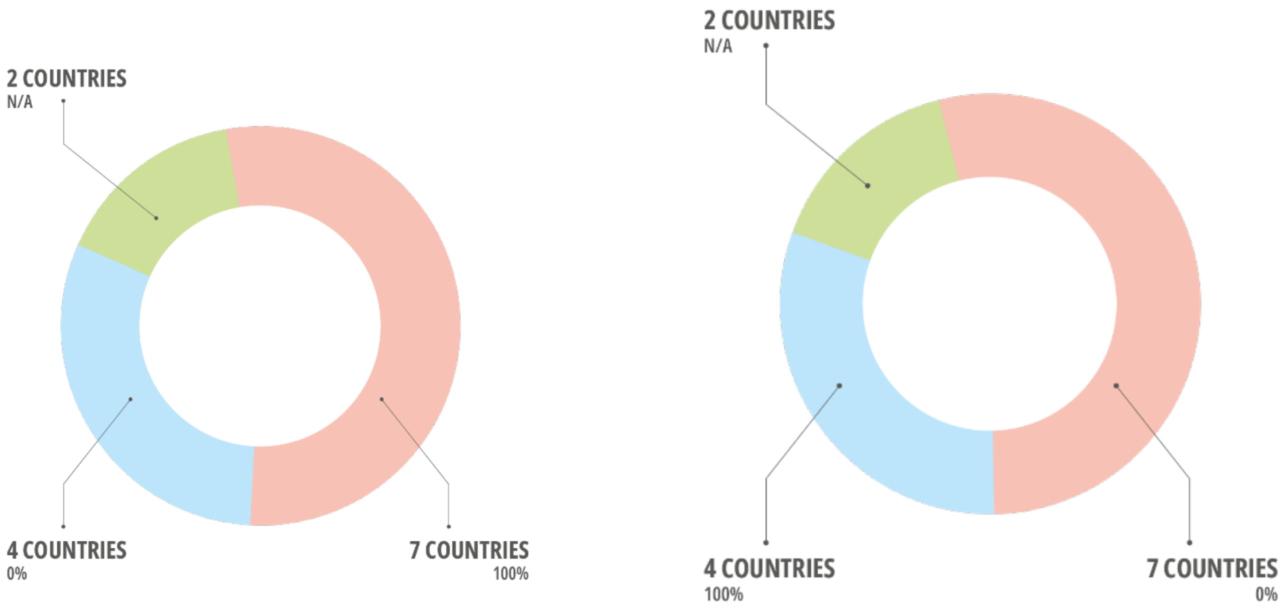
National cybersecurity strategies are usually accompanied by national action plans designed to implement the strategy pragmatically within the MS, and sometimes imply the creation of working groups and cross-sector cooperation.

2.2.2 Assessment of national action plans (sub-dimension 2.2)

As illustrated in Figure 6, the majority of the MS (7) consulted had set a cybersecurity multiannual action plan in order to ensure the implementation of the NCSS. These countries, therefore, display a maturity level equal to 100 %. Among these countries, only 4 reported that their action plan specifically mentioned actions regarding cybersecurity education for the primary and secondary levels. Despite the creation of a national action plan, 1 country reported difficulties in the concrete implementation of the latter. In fact, the organisation in charge of cybersecurity education often faces reluctance from the ministry of education to implement the action plan (as mentioned in previous sections), often due to insufficient resources. Moreover, the shortage of trained teachers in primary and secondary schools is an obstacle often put forward. Indeed, as further developed in the 'Operational dimension, Section 2.3', it can be difficult to deliver courses in schools, as advocated by the NCSS and the corresponding action plan, due to teachers' lack of cybersecurity skills and knowledge, and the absence of IT infrastructure. Because of these obstacles, national action plans may remain unimplementable in some countries.

In all, 4 countries remain at the 'Non-existent' maturity level, with no action plan foreseen or implemented.

Figure 6 – Member States' maturity on the implementation of a cybersecurity action plan – and portion of cybersecurity action plans specifying primary and secondary education



Source: Authors' elaboration (data analysis based on the sampled countries, 13 in total).

Aside from action plans theoretically centralising all country initiatives, all represented countries have stand-alone initiatives in place, managed by different stakeholders and sometimes involving cross-national cooperation (e.g. the Cybersecurity Challenge). In fact, in each country there are various efforts that focus on different age groups, on raising awareness and on building content for schools, but these initiatives may not be connected to a specific national action plan.

Figure 7 – Country example of cybersecurity initiatives at the national level

In Czechia, many cybersecurity education initiatives were initiated during the COVID-19 pandemic. All initiatives are reported and explained in the catalogue of cyber-prevention that presents 256 initiatives. Some initiatives are local (connected mainly to schools) and some are regional and cross-regional. In total, there are 15 initiatives conducted at the national level. Most of them are managed by non-governmental organisations (NGOs).

The catalogue includes **three types of material**:

- programmes for students;
- programmes for teachers and parents;
- supporting materials and methodologies for experts in education.

The catalogue is organised via the filters listed below:

- target groups (e.g. teachers of primary and secondary schools);
- formats of the materials (e.g. online / hard copy / school books);
- regions, as the educational initiatives are left for the schools to implement.

A limitation of this catalogue is the **lack of supporting accreditation**. In fact, the Ministry of Education is not responsible for the accuracy and alignment of the materials with the national requirements on education and curricula.

In parallel with this catalogue, one of the main outputs of the national programme was the **National Cybersecurity Competition** involving 7 000 students. This initiative targeted students aged from 9 to 25 years old. Participants gained new skills and experience, and how to quickly adopt a 'safe internet' behaviour.

The website of the National Cyber and Information Security Agency includes **materials for all stakeholders** involved in the health and medical sector, law enforcement and education.

Digital skills Cyberfairytales. This initiative aims at turning a 'real world' set-up into a virtual world to raise awareness on how to behave in a virtual environment.

Another initiative is called Czechitas, which focused on girls who are in interested in programming and digital skills. Around 1 000 young girls are involved, starting from high school.

In addition to actions addressed to schools and teachers, NSCCs may include recommendations and guidance relating to the creation of cooperation groups, as presented in Section 2.2.3.

2.2.3 Assessment of national initiatives to foster cooperation (sub-dimension 2.3)

Cooperation may include collaborations at the national level across the government entities, but also the participation of municipalities, academia, private-sector stakeholders and NGOs.

Figure 8 – Country example of national governance and cooperation across education and cybersecurity stakeholders

Cybersecurity education actions conducted in Luxembourg are aligned with the National Cybersecurity Strategy IV. The strategy mentions the need for cybersecurity education and refers to the BEE SECURE governmental initiative as one of the drivers toward a better cybersecurity education.

Operating since 2010 under the name BEE SECURE, this government initiative is coordinated by the National Youth Service (*Service National de la Jeunesse*, SNJ). Participation on the part of the government is ensured by the Ministry of Education, Children and Youth, the Ministry of Economy and the Ministry of Family and Integration. BEE SECURE is operated by the SNJ in collaboration with consulting service KJT, and in partnership with Luxembourg House of Cybersecurity, the Grand-Ducal Police and the Public Prosecutor's Office of the Grand Duchy of Luxembourg. Thanks to its practical cybersecurity experience in Luxembourg and its established network of partners, BEE SECURE is able to contribute in a concrete way to the empowerment and education of young internet users.

In order to carry out its mission (based on four pillars), the BEE SECURE initiative relies on many partners, such as SCRIPT (*Service de coordination de la recherche et de l'innovation pédagogiques et technologiques*), the entity in charge of promoting, implementing and coordinating projects, initiatives and research aimed at educational and technological innovation throughout the education system in Luxembourg. In the SCRIPT department of initiatives, a new programme called Level Up focuses on federating and promoting competitions and challenges that address students and have pedagogical or educational objectives. In this respect, one of the topics of the Level Up initiative is cybersecurity, where a new competition was introduced in 2023. This complements the role of the SNJ as coordinator of BEE SECURE and main stakeholder in non-formal education. The SNJ is the stakeholder that brings innovation to education on cybersecurity.

As a general trend, cybersecurity education cooperation and initiatives usually follow a bottom-up approach, often led by associations and NGOs. The aim of such cooperation is usually to create synergies among various stakeholders, including teachers. Considering this approach, teachers would have the possibility to express their needs (e.g. training material, schoolbooks, infrastructure) and share challenges and best practices. As cybersecurity is a fast-evolving topic, different stakeholders with different skill sets would benefit from working collaboratively. For instance, schoolteachers would need to frequently update their course content to cope with technology evolution. They would surely benefit from the support and knowledge-sharing practices from private-sector stakeholders who confront this evolution on a daily basis.

2.2.4 Good practices on strategic aspects (dimension 2)

Table 4 – Good practices identified at the national level (Strategic dimension)

Good practice		Sub-dimension	Example from a Member State	
1	Enhance national, regional and municipal cooperation	Cooperation and supporting initiatives	🇧🇪	As Belgium's national authority on cybersecurity, the role of the Centre for Cybersecurity is to coordinate with the different regions that are responsible for education. With the creation of the national coordination centres – and therefore the NCC-BE – an explicit role was assigned to improve coordination within the national communities. The NCC-BE will continue to build relations with the different regions and regional governments by providing them with expertise, resources, support and (information on) funding opportunities. A nationally supported strategy will ensure an increase in cybersecurity maturity.

2	Create cooperation between public and private organisations and across industries	Cooperation and supporting initiatives	🇷🇴	The cooperation with stakeholders of the private sector (Romanian Association of Banking) and the Romanian Police led to the creation of a platform for children to test their cybersecurity knowledge. This cooperation is backed by the law that established the National Cyber Security Directorate, which calls for multiple ministries and institutions to be involved and collaborate at different levels.
3	Create opportunities to favour and upgrade knowledge and skills sharing	Action plan and supporting initiatives	🇩🇰	In Denmark, the Cybersecurity Challenge is carried out yearly to select 10 participants (between the ages of 15 and 25) for the European Cybersecurity Challenge and the Cyberskills project. The latter aims at increasing knowledge and interest in cybersecurity among young people. Activities are carried out and largely funded by the private sector (EUR 5 million for the next 3 years) to support the building of a community amongst young people. The objective of the activities is to increase cybersecurity knowledge and skills. There are currently around 2 000 members in the Discord server created for the Cyberskills project. The activities of the two projects include the distribution of high-quality material for teachers, online training sessions for all ages and levels of expertise (2 000 users have used the training in the last spring session) and events with local clubs and experts. In some schools, the teaching materials are integrated into secondary school computer science courses.
4	Training of teachers and upgrading of students' skills	Cooperation and supporting initiatives	🇮🇹	In Italy, the CyberHighSchools programme, promoted by the Cybersecurity National Lab (a collaboration involving most of the universities in the country), has established a network of secondary schools with active involvement from both students and teachers. Currently, there are more than 500 schools in the programme. The teachers at these schools attend cybersecurity training courses which are currently offered at two levels: basic and advanced. In this way, universities assist in 'teaching the teachers' and approximately 1 000 teachers have participated so far. Students at these schools are provided with courses taught by their teachers and are also encouraged to participate in the OliCyber competition for high school students. More than 4 000 students took part in the selection process for the 2023 OliCyber competition, and 900 of them were admitted. Out of these, 360 had the opportunity to attend a training camp and 100 reached the finals. The activities also encompass a competition specifically designed for high school girls with no prior technical background, aiming to help reduce the gender gap in the field.

2.3 MATURITY AT THE OPERATIONAL LEVEL (DIMENSION 3)

This subsection aims to provide a more detailed assessment of the **operational dimension** governing the implementation of cybersecurity education. It will build on the insights collected through the detailed desk research on the 27 MS and the detailed insights shared by the 13 countries represented within the data collection activities and result computations within the theoretical framework. Additionally, good practices identified through interviews and/or the detailed desk research will be highlighted in Section 2.3.3.

As per the theoretical framework presented in Section 2.2, the 'operational' dimension is divided into two sub-dimensions: **Provision of cybersecurity education and Monitoring mechanism**

and/or framework. The EU average is at 78 % when it comes to providing primary and secondary pupils with cybersecurity education, regardless of the methods employed. Referring to the 13-country sample of this study, the EU displays an 'Establishment' maturity level, which means that while sometimes lacking formal and uniform national approaches, most of the MS manage to provide pupils with relevant cybersecurity knowledge.

An important aspect of cybersecurity education and the underlying initiatives is the regular control, monitoring and assessment of their effectiveness. The EU's maturity level with regard to monitoring and evaluation practices for cybersecurity education initiatives remains ad hoc or in its infancy (maturity level: 'Initial/ad hoc', 23 %).

Each sub-dimension is detailed in the below section as follows: Provision of cybersecurity education, Section 2.3.1 and Monitoring mechanism and/ or framework, Section 2.3.2.

2.3.1 Assessment of initiatives for providing cybersecurity education (sub-dimension 3.1)

In all consulted countries (13), cybersecurity courses are delivered to primary and/or secondary schools wheretwelve (12) of them reported that cybersecurity is included in either primary or secondary school curricula. However, the level of maturity on the topic differs across MS. The majority of the countries stands in the 'Initial/ad hoc' maturity level, where cybersecurity topics are only provided on a voluntary basis. This means that schools are either not obliged to deliver courses on cybersecurity or that they are optional. Additionally, classes may be delivered to pupils, but they are not evaluated (i.e. pupils do not take exams on cybersecurity).

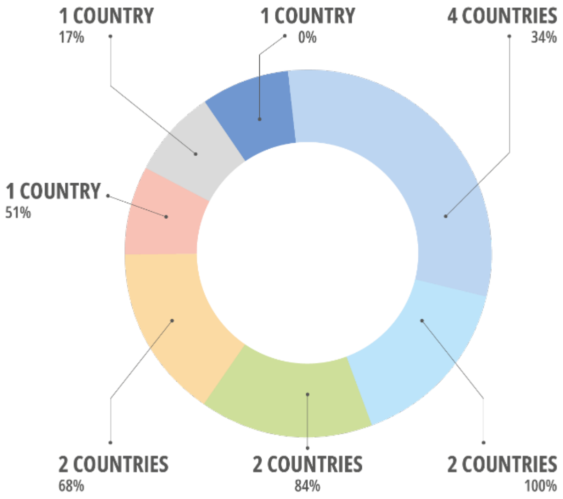
A major blocking point limiting the adoption of cybersecurity courses in EU schools reported by the MS is the knowledge gap faced by primary and secondary schoolteachers. Because of this, the quality of classes usually varies across schools, resulting in unequal chances for pupils to learn about cybersecurity topics. Schoolteachers tend not to be trained and equipped (i.e. insufficient training materials and/or IT infrastructure) enough to feel comfortable in delivering cybersecurity courses. To cope with this problem, NCSS and ministries of education (sometimes with the support of private-sector stakeholders) provide training materials addressed to teachers, i.e. following a 'train the trainer' approach. Some countries have also launched working groups in order to share experience, ideas on relevant cybersecurity topics and use cases. Some NCSS representatives reported facing a high demand of training, bootcamps and material from motivated schoolteachers willing to learn and teach about cybersecurity, and from school directors eager to upgrade their curricula.

Additionally, the 4 most advanced countries (i.e. with maturity levels equal to 100 % and 84 %; 'Optimisation/Adaptions' and 'Establishment' respectively) have mandated cybersecurity courses in curricula for the secondary and primary levels (more in-depth courses for the secondary level). It was also observed that in most countries, the school system offers different paths for pupils. Cybersecurity tends to also be mandatory for certain specialised academic paths relating to applied sciences, digital sciences or IT in general.

The MS showing an 'Early definition' maturity level shared that cybersecurity per se is not currently mentioned in the curricula for primary and secondary schools, however 'Digital literacy' is. The existence of topics touching upon cybersecurity in these classes strongly depends on the teacher's motivation and knowledge.

Lastly, only 1 country among the 13 sampled countries stated having no cybersecurity or digital-related courses in its school curricula.

Figure 9 – Member States' maturity on the inclusion of cybersecurity topics in primary and secondary education curricula



Source: Authors' elaboration (data analysis based on the sampled countries, 13 in total).

As an illustration of a bottom-up and gradual approach for including cybersecurity into school curricula, the pilot organised by Ireland is presented in Figure 10. One should note that regardless of countries' maturity level, all MS have produced materials addressed to teachers and pupils in different formats and available in multiple sources, to ensure accessibility and demographic coverage.

Figure 10 – Country example of operational implementation of cybersecurity education actions

In Ireland, a pilot project aiming to strengthen cybersecurity in education was initiated based on a policy aligned with the National Cybersecurity Strategy. The initiative includes a representative sample of different schools (around 20 schools of different levels, geographical coverage and school types). These schools were invited on a voluntary basis to deliver cybersecurity classes to pupils. After the end of the second phase (by the end of 2024), the aim is to expand the scope of the pilot project to 50–100 schools.

The pilot project introduces the topic of cybersecurity as a subject in the schools participating in the pilot. Therefore, it not yet a part of the national curriculum, however the aim of the pilot is to favour its expansion to more schools in the near future.

The topics covered in the courses are up to the teachers, both for primary and secondary schools. In primary schools, the topics usually focus on raising awareness of the risks and threats of cybersecurity, along with cyber hygiene. For secondary education, more in-depth topics are covered, such as:

- cyber hygiene;
- role of regulation;
- cybersecurity in society;
- ethics and behaviour;
- raising awareness of risks and threats of cybersecurity;
- practical aspects, malware, etc.

The Irish initiative also implies the development and provision of materials for primary, secondary and tertiary education. A bottom-up approach is followed to share ‘hands-on’ training and ensure teachers are equipped to train pupils, and to raise awareness among students.

Age-appropriate material is produced in different formats, to ensure access to any teacher and pupil (e.g. research projects to be executed by pupils, online and open-source resources, access to practical materials, webinars and training days).

Besides the consideration of cybersecurity topics in curricula at the national level, the **organisation of challenges, events and bootcamps** was frequently mentioned as an efficient and motivating initiative to promote cybersecurity topics among pupils. In fact, either autonomously or in anticipation of the European Cybersecurity Challenge organised by ENISA, most consulted countries reported having organised national Cybersecurity National Challenges. These events gathered between 200 and 2 000 pupils and sometimes involved cross-border cooperation. The events provided opportunities to raise awareness among pupils, generate interest for cybersecurity topics and classes and share training materials and online content.

2.3.2 Considerations on the implementation of an evaluation mechanism (sub-dimension 3.2)

In this context, an ‘evaluation mechanism’ means a framework that would help MS and responsible authorities assess the performance, efficiency and coverage of implemented actions and initiatives.

Only 2 countries (showing a ‘Optimisation/adaptions’ maturity level) reported having set monitoring measures, even if they are not part of a coordinated monitoring process for the overall action plan.

In one of the consulted countries, teachers usually receive quantitative feedback from the participation of pupils in their modules. Additionally, a final report relating to the overall implementation of cybersecurity in education will be published, which should include quantitative assessments of the participation of pupils across the participating schools.

The other national authority reported a monitoring framework at the national level. However, every stakeholder tries to promote cybersecurity awareness in the most effective way. Therefore, the monitoring is carried out separately. This authority, which oversees EU projects, has to meet key performance indicators that are linked to brand awareness and the reach of social media campaigns. Lastly, the organisation usually shares questionnaires to obtain qualitative feedback on initiatives, teaching material, events and publications. As of today, around 1 300 training sessions are carried out yearly and qualitative evaluations are obtained from the participants (students) and teachers, educators and trainers.

2.3.3 Good practices on the operational aspects (Dimension 3)

Table 5 – Good practices identified at the national level (Operational dimension)

Good practice		Sub-dimension	Example from a Member State	
1	Apply a 'train the trainer' approach by training schoolteachers	Provision of education	🇮🇪	In Ireland, best practices have been identified in relation to providing guidance and training to the teachers, following a 'teaching the teachers' approach. Additionally, teachers are involved in developing the course, as the course would need to get their approval. By involving teachers in the development of the course, their buy-in is secured.
2	Ensure accessibility of cybersecurity courses by providing different course formats	Provision of education	🇧🇪	In Belgium, there are various options available to train students to reach cybersecurity learning goals. ● Traditional in-class, instructor-led teaching involves the use of books with associated e-learning content created by educational publishers that incorporate the official educational objectives. Cybersecurity is then typically included via blended learning in the ICT course that many schools have in their curricula. ● Regional and national initiatives provide educational cybersecurity content targeted at young pupils. This often involves some form of gamification combined with a digital learning platform. Examples are the EDUbox Cybersecurity and the international Pix platform that were co-funded by the European Commission.
3	Digital skills assessment	Implementation evaluation mechanisms	🇫🇷	The French Ministry of Education uses the Pix platform to assess digital skills of the population. The platform was built in collaboration with ANSSI and Cybermalveillance.gouv.fr. The platform evaluates students' skills based on five domains (the fourth being 'Protection and security'). The test is based on the EU Digital Skills Assessment Tool and helps understand the level of digital skills of French students and adapt their cybersecurity education experience.

3. RECOMMENDATIONS

This section provides **recommendations** aiming to support the development and provision of materials on cybersecurity education. For **each maturity level** defined in our maturity assessment framework and drawing from the inputs received in the targeted consultation, the team identified and listed recommendations for cybersecurity education-related actions and activities to be developed by the MS. These recommendations aim to provide guidance to develop, reuse and deploy appropriate materials, activities and campaigns in primary and secondary schools. Moreover, the recommendations provide the relevant stakeholders with guidance for setting the objectives, addressing the needs of students and maturity gaps.

3.1 RECOMMENDATIONS ON THE GOVERNMENTAL LEVEL (DIMENSION 1)

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
1. Incorporate cybersecurity within one of the pillars of a greater policy focused on media literacy.	x	x			
2. Involve the Ministry of Education and academic and research networks and institutions in the creation and implementation of general and broad curricula to ensure that all students attain the same skills and in the development of activities that will foster cybersecurity education.		x	x	x	
3. Make cybersecurity education binding and a high priority of the government.				x	
4. Have the Ministry of Education help provide access to EU grants and private initiatives for funding of cybersecurity education.			x	x	x
5. Be part of and develop a communication strategy alongside the strategy on cybersecurity education.				x	x

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
6. Implement pilot projects in a number of schools based on the national strategy's objective to strengthen cybersecurity in education.			x		
7. Account for the maturity level of schools that has been previously measured, in compliance with EU and/or international frameworks.			x	x	x

3.2 RECOMMENDATIONS ON THE STRATEGIC LEVEL (DIMENSION 2)

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
1. **Engage teachers in course development and consider the utilisation of a bottom-up and 'teach the teacher' approach to support the concrete implementation of cybersecurity education and ensure their commitment and buy-in.**		x	X		
2. **Collaborate with universities to offer cybersecurity courses to primary and secondary school students, and simultaneously certify teachers to validate their competency in teaching cybersecurity.**			x	x	
3. **Provide support for projects aimed at adapting existing cybersecurity content for effective classroom integration.**		x	x		

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
4. **Provide schools the opportunity to schedule certified cybersecurity trainers for in-school sessions.**	x	x	x	x	x
5. Build a continuous and coherent plan and learning path that starts from primary school and combine cybersecurity with the formal qualification of teachers.			x	x	x
6. **Introduce cybersecurity concepts through interactive challenges and gamified e-learning resources.**		x	x	x	
7. **Integrate essential cybersecurity skills and concepts into digital competences and skills courses and in other educational areas (e.g. economics, social studies).**			x	x	
8. **Emphasise understanding, practical know-how, prevention and the ability to self-assess risky online behaviour and apply safety measures from a positive perspective ('what to do' instead of 'what not to do').**			x	x	
9. **Develop national-level targets while granting schools autonomy to select materials and content for cybersecurity education.**	x	x	x	x	x
10. Consider the development of a working group that includes stakeholders of the education ecosystem and their involvement in the implementation and extension of cybersecurity education initiatives.		x	x		
11. Cooperate with the private sector and universities in developing training materials for primary and secondary school students that are aligned with current trends.	x	x	x	x	x
12. Involve students in promoting and teaching cybersecurity to other students (peer learning).		x	x		x

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
13. **Promote comprehensive cybersecurity education and career paths by partnering with industry-led programmes and launching media-backed campaigns to highlight cybersecurity professions.**			x	x	x

3.3 RECOMMENDATIONS ON THE OPERATIONAL LEVEL (DIMENSION 3)

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
1. Engage in cybersecurity activities carried out in other MS.	x	x	x	x	X
2. **Involve external experts and/or universities in the facilitation of the cybersecurity courses/classes.**	x	x	x		
3. **Pilot test the implementation of cybersecurity curricula before mandating its inclusion.**			x	x	
4. **Introduce mandatory hours of instruction on cybersecurity awareness.**				x	x
5. Provide a certification after the completion of cybersecurity courses.			x	x	

Recommendations	Non-existent (Level 1)	Initial/ad hoc (Level 2)	Early definition (Level 3)	Establishment (Level 4)	Optimisation/ adaption (Level 5)
6. Develop a monitoring framework centred on the effectiveness of implemented cybersecurity education initiatives, using surveys to assess their impact.				x	x
7. Introduce a roadmap to encourage and guide students to pursue a cybersecurity career.				x	x
8. Consider different requirements based on school type and the geographical and social background of pupils when implementing curricula.				x	x
9. Build and refer to advisory boards which engage with various cybersecurity stakeholders, in particular the ones who have access to very large online platforms.					x

3.4 RECOMMENDATIONS AND EXPECTATIONS FROM THE MEMBER STATES ON THE ROLE AND ACTIONS TO BE TAKEN BY ENISA

A set of recommendations and expectations shared by the MS introduces how ENISA can help increase the maturity level of cybersecurity education in Europe. The role and actions proposed by the MS were distributed per dimension of the maturity assessment model.

Dimension 1 – Governmental level

- Support the dissemination of information across the EU and the implementation of policies and programmes to support the cyber resilience of citizens.
- Provide a harmonised framework for curricula for both primary and secondary school levels. These should be accompanied by quantitative key performance indicators that the MS should track.
- Be the main liaison and/or organiser of events between different MS and stakeholders of the cybersecurity sector who are involved in the education sector.

Dimension 2 – Strategic level

- Provide guidance and support on how to address the challenge of finding, upskilling and maintaining teachers with cybersecurity knowledge at both the primary and secondary school levels.
- Promote the sharing of tools, assessment frameworks, trainings and best practices.
- Provide a centralised platform to share and promote initiatives and projects (tools, materials, expertise, glossary) developed by the MS relating to cybersecurity education, that can be repurposed by teachers.
- Offer direction regarding the various aspects of cybersecurity suitable for exploration with primary and secondary school students.

Dimension 3 – Operational level

- Develop and provide training programmes that can be repurposed and used by teachers.
- Consult children and teenagers in the development of cybersecurity material and activities based on their experiences.
- Focus on raising awareness beyond the school environment (real-life scenarios) and on the preparation and recruitment of the next generation of cybersecurity specialists.
- Consider the addition of cybersecurity to cultural or linguistic exchanges done at the school level.

4. CONCLUSION

The aim of this ENISA study on assessing the maturity of cybersecurity education was to present the current outlook in the MS. For this purpose, a maturity model was selected and designed to meet the objective of this study. This model is structured into key dimensions and objectives, which are assessed using a series of indicators. Its ultimate aim is to assign a level of maturity to each MS in the field of cybersecurity in education and to gain a better understanding of the advances and challenges in the EU. In summary, the main findings reveal that, based on data obtained from stakeholders in 13 countries, **MS have an average maturity level of 66 % in cybersecurity in education**, corresponding to level 4 ‘Establishment’.

The first tier of the maturity model was designed to comprehensively assess the strategy for ensuring, promoting and implementing cybersecurity education across MS. This tier further dissects the ‘Establishment’ level, encompassing three key dimensions: **Governmental (70 % EU average), Strategic (64 % EU average) and Operational (63 % EU average)**. These figures and the breakdown of the data presented in the report reveal that MS have taken significant steps to follow European cybersecurity directives (NIS) and execute actions aligned with existing national and regional efforts that aim to support students in acquiring knowledge in cybersecurity. However, the implementation of curricula and initiatives continues to progress at a moderate pace due to the numerous stakeholders involved in the operationalisation of the education sector from top to bottom.

Additional factors that add to the challenges of implementing cybersecurity curricula and classes stem from the difficulty in cooperating with the various entities involved and the priorities set at the governmental level that often do not leave space for cybersecurity-related topics to be included in the curricula. Stakeholders interviewed for this study also proposed an alternative approach, involving a bottom-up strategy in which teachers actively participate in cybersecurity activities organised by national and local entities. However, this approach introduces other challenges: the need to have enough adequately prepared teachers for instructing this topic and ensuring they have access to adequate materials.

Nevertheless, MS have shown a **high level of voluntary engagement in initiatives aimed at primary and secondary school students** with the involvement of schools. These initiatives, requiring fewer agreements and restructuring of the existing curricula, have proven to be an opportunity to introduce the cybersecurity topic and foster the development of academic content to support the integration.

It is important to consider these and various other challenges when interpreting the findings in this study. The MS surveyed do not encompass the entire EU spectrum, and the stakeholders interviewed often presented various involvement levels across the three dimensions of the maturity model examined during this study, requiring follow-up with additional entities and bodies. These factors have led to certain data points being less representative and the exclusion of two MS from the analysis.

Integrating cybersecurity into national education curricula within the education policies at the Member State (MS) level is progressing at a moderate pace, therefore highlighting the need for a strategic and coordinated approach to engage educational stakeholders in MS. ENISA is systematically working with these stakeholders and develops relevant work that may assist in gradually integrating more cybersecurity content into national curricula, ensuring a comprehensive and unified effort to enhance cybersecurity education across the EU.

TP-09-24-366-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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-674-3
doi: 10.2824/3832