CONCORDIA Governance model for a European Education Ecosystem for Cybersecurity

This report was developed under the CONCORDIA project[1] under the Task 3.4. and received contribution from the REWIRE project[2]. It is envisaged that the REWIRE project will build on the proposals put forward by this report and suggest more concrete elements to be considered for building the European Education Ecosystem for Cybersecurity.

Publication date	*10.03.2023*
Dissemination level	*Public*
Editor	*Felicia Cutas (EIT DIGITAL)*
Contributors	*Felicia Cutas (EIT DIGITAL)* *Argyro Chatzopoulous (TUV TRUST IT)* *Manos Athanatos (FORTH)* *Despoina Antonakaki (FORTH)*

[1] This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830927.

[2] https://rewireproject.eu/

Table of Contents

1. Introduction

Europe continues facing several challenges in terms of cybersecurity education. From insufficient awareness raising, persistent skills gap and a lack of gender equality in the sector to not enough interaction between the actors at all levels, lack of comprehensive sharing platforms and of willingness to share knowledge. Efforts were put in place both at national and European levels by defining specific objectives linked to education in cybersecurity and governance models for bringing together the relevant actors to address the challenges at national levels. Yet, to efficiently address the challenges at European level, a transnational cooperation between Member States would be paramount. The cooperation model would need to be defined in such a way to encourage EU Member States and all actors to contribute to addressing the common European challenges of the cybersecurity education ecosystem.

There are several definitions for governance, some varying or being adapted to better fit a specific domain.[3] Aguilera introduces the subject of governance in the context of an organization as "Corporate governance may be defined broadly as the study of power and influence over decision making within the corporation." This document aims to provide an overview and recommendations on the Governance of the European Education Ecosystem for Cybersecurity (EEEC). This ecosystem is composed of different elements and different players, residing at different levels (local, national, European). This ecosystem is a complex system as introduced by Complexity theory[4]. Specifically, a Complex system is a system that "poses several challenges as a particular system can no longer be examined in isolation" and the study of complex systems "requires a step back to look at how the various interconnections can for, a coherent whole"[5].

To this effect and following the basic instructions of Complexity Theory, the analysis of the European Cybersecurity Education Ecosystem should be split into three parts. The first part involves the overview of the ecosystem and the understanding of challenges, activities, members, goals and risks. The second part involves the identification of the various players of the European Cybersecurity Education Ecosystem and their interconnections as well as current governance models employed in similar or related subjects. The third part involves the condensation of the analyzed information in order to derive recommendations and conclusions.

Specifically, the CONCORDIA project carried out the following activities:

- Identification of the challenges of the European Cybersecurity Education ecosystem at European and national level (Chapter 2)
- Identification and review of other cybersecurity / education governance models (Chapter 3.)
- Description of the efforts and activities implemented by the CONCORDIA project to promote cooperation and effective cybersecurity education governance (Chapter 4)
- Recommendations on how a European Education Ecosystem for Cybersecurity related governance model could be organised and function (Chapter 5)

The Governance model proposed by CONCORDIA aims at supporting the European Cybersecurity Competence Centre endeavor in building and engaging with the Education related community, for the benefit of all the actors of the ecosystem.

[3] Aguilera, Ruth V. and Jackson, Gregory(2010) 'Comparative and International Corporate Governance', The Academy of Management Annals, 4: 1, 485 — 556, First published on: 05 July 2010 (iFirst)

[4] "Complexity theory provides an understanding of how systems, such as the economy and global corporations, grow, adapt, and evolve. It explains how the relationships between members of these systems give rise to collective behavior and sheds light on how a system interacts with its environment."

[5] Educational Research and Innovation. Education Governance in Action. Lessons from Case Studies. https://doi.org/10.1787/9789264262829-en

2. European Cybersecurity Education ecosystem challenges

2.1. Challenges at European level

The EU overall objective in terms of cybersecurity is to ensure the Union's sovereignty and resilience[6]. There is no doubt that Education can and should play an important role in achieving this objective. The scarcity of skilled workforce in the cybersecurity domain, which is persisting, implies that the workforce needs to be enlarged through activities and policies at national and EU level, aiming on training and education in the field of cybersecurity. At the EU level, the current Digital Europe Work Programme includes as one of the strategic objectives the "Advanced Digital Skills" and is looking into financing actions related to both (1) specialized education programmes or modules in key capacity areas like data and AI, cybersecurity, quantum and HPC, and (2) upskilling of the existing workforce through short trainings reflecting the latest developments in the above key capacity areas. Yet, these actions will pay off only in the medium term and it is difficult to estimate now the impact at national level. On the other hand, the situation seems to differ from one member state to another. As flagged in the CONCORDIA Courses assessment report[7]countries with a great number of offered cybersecurity related courses (thus with presumably more skilled people) are not necessarily the ones also looking for hiring them and the other way around.

As part of the project, and in the context of the CONCORDIA Cybersecurity Roadmap for Europe[8], a specific education related chapter was developed. The CONCORDIA Education & Skills roadmap[9] is looking into the challenges related specifically to the cybersecurity professionals and their needs for up-skilling or re-skilling. It complements the efforts of the other pilot projects (SPARTA and ECHO) which are looking into cybersecurity education at university level. The document describes a set of challenges and recommendations to address the identified challenges. It offers a view on the recommendations in terms of initiating the recommendations' actors, and the actors impacted by the recommendations once implemented. It also proposes a timeline for the implementation of the recommendations. Between the most important challenges described in this paper we could mention: (C1) the skills gap is persisting, (C2, C3) it is difficult to understand and to see the trainings big picture, (C4) there is a heterogeneity of the terminology related to competencies , (C7) there is a different level of cybersecurity preparedness, (C8) there is a lack of cybersecurity culture, (C9) cybersecurity appears to be gender biased. While specific recommendations are put forward to address these challenges, one recommendation is covering them all: (R12) Establish an inclusive governance model for the European education ecosystem.

Building on the outcomes of the 4 pilot projects CONCORDIA, SPARTA, ECHO and CyberSec4Europe, the REWIRE project went a step forward and looked into the skills shortages, gaps, and mismatches affecting cybersecurity education by performing a Political, Economic, Social, Technological, Legal, and Environmental evaluation those results were captured in the REWIRE PESTLE analysis[10]. This analysis offered an overview of the cybersecurity education environment from multiple perspectives. The results of this analysis highlight 31 different factors affecting cybersecurity education at a European level. These factors were further analysed from the specific perspectives of 11 European countries and the pilot projects. The analysis flags, among others, a governance shortage, i.e., a lack of European coordination and cooperation, which was strongly identified by all countries and pilot projects involved in this analysis. Furthermore, asocial network analysis, conducted as part of the same task of the REWIRE project, flags the identification of four challenges (1) failure of stakeholders to cooperate,

[6] https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[7] https://www.concordia-h2020.eu/wp-content/uploads/2020/04/CONCORDIA-AssessmentOfCoursesT3.4-ForWebsite.pdf
[8] https://www.concordia-h2020.eu/concordia-reports/
[9] https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf
[10] https://rewireproject.eu/wp-content/uploads/2022/04/R2.1.1-PESTLE-analysis-results_FINAL-v1.1_compressed.pdf

2) lack of a skills framework, 3) lack of training resources, and 4) low level of societal interest in cybersecurity.

On their side, the European Cybersecurity Organisation (ECSO) made an analysis of the different Education related challenges at European level and published them end of 2022 under the blog on Unlocking our potential: Cybersecurity Education and workforce needs in Europe[11]. The author mentions that "There is no better time than the present to leverage the collaborative spirit of the European cybersecurity community to deliver practical solutions and initiatives that can have an impact "on the ground". Education being a national prerogative, and inherently linked to skills development, there is a need to work closely with national entities and education and training providers to build up joint, pan-European approaches to harmonising cybersecurity education curricula and tackling the skills or, more concretely, workforce gap."

Based on ECSO different analysis, the Cybersecurity education ecosystem has an increased complexity due to:
a) the nature of cybersecurity. Cybersecurity is a complex domain encompassing different technologies and use cases[12] (e.g. AI and Big Data Analytics, Cloud, Edge and Virtualization etc.), different research domains (e.g. Assurance, audit and Certification, Legal Aspects, Data Security and Privacy etc.) in various sectors (e.g. Health, Public Safety, Space, Energy etc.). Cybersecurity is not a purely technological subject nor a purely organizational one. This means that the skills and knowledge by the cybersecurity professionals are also diverse. To further add to this complication, cybersecurity is a fast-evolving subject. Meaning that challenges arise also from the need to keep the knowledge and skills provided (within education, awareness, and training activities) up to date and current.
b) the increased number and diversity of the "players". The issues identified within a) also give rise to an increased number of interested parties that need to collaborate within education, awareness, and training activities. Cybersecurity education is not a subject restricted only to academic institutions or training providers without the collaboration with technology providers. Technology is necessary for the implementation of the lab environments to the presentation and usage of specific solutions and tools in theory and practice. As pinpointed by the (ISC)[2] [13] Cybersecurity Workforce Study 2022, "From 2021 to 2022, practical skills and experience have grown into being more important qualifications for those considering employment in the cybersecurity profession."
c) the fact that each member state has a different awareness and maturity level and thus needs regarding cybersecurity education. The DESI[14] index includes country profiles which support Member States in identifying areas requiring priority action as well as thematic chapters offering a European-level analysis across key digital areas, essential for underpinning policy decisions. The indicator "Above basic digital skills", for individuals aged 16-74, shows the "individuals with 'above basic' digital skills in each of the following five dimensions: information, communication, problem solving, software for content creation and safety". Although this indicator is not one directly connected with cybersecurity, it could be used to guide a rough conclusion on the subject since it incorporates the safety component. This indicator as displayed in Fig.1. shows the different European Countries having a great variety (in average values). Specifically, the Netherlands show a 51,8% percentage of the individuals having Above basic digital skills whereas this percentage for Bulgaria is 7,8% and Romania is 8,7%. The average value for the European Union is 26,5%.

[11] https://ecs-org.eu/unlocking-our-potential-cybersecurity-education-and-workforce-needs-in-europe-2/
[12] https://cybersecurity-atlas.ec.europa.eu/cybersecurity-taxonomy
[13] https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[14] https://digital-strategy.ec.europa.eu/en/policies/desi

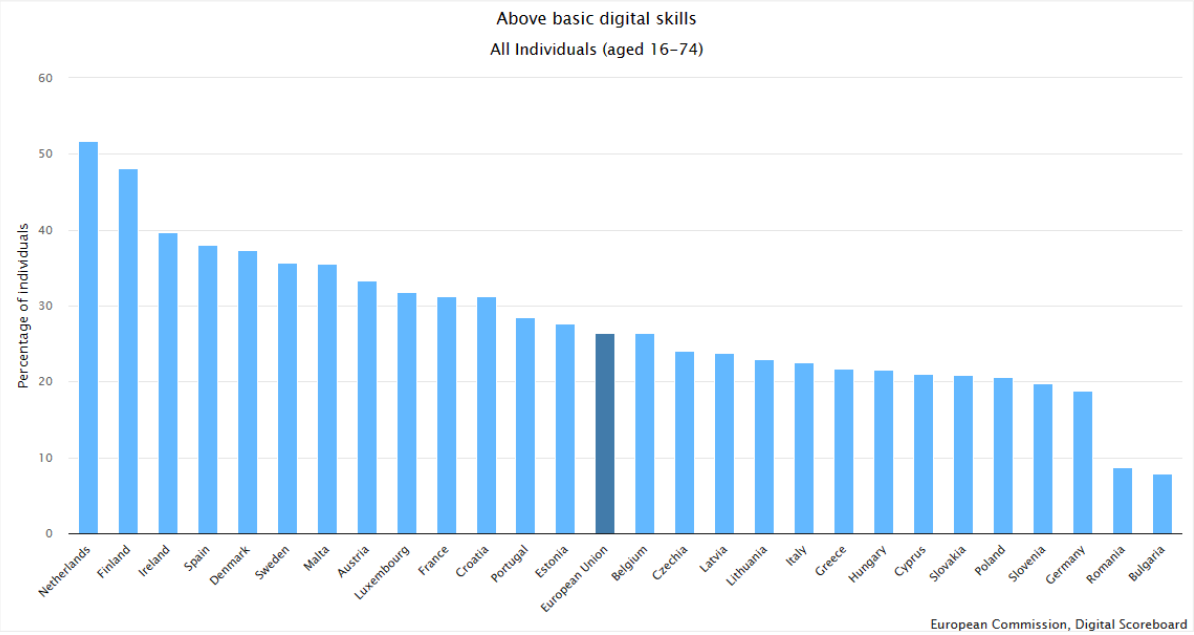


Fig. 1. European Commission Digital Scoreboard

The identified challenges for Cybersecurity Education from the publications in ECSO indicate that there is:

- a lack of ability to scale up national initiatives
- an increased need for easier mobilization of resources
- a challenge in ensuring that education is fit for purpose and that graduates of cybersecurity university programmes are equipped with the skills and knowledge necessary to meet the requirements of industry
- a lack of scalable and flexible solutions to quickly allow organisations to train and upskill their workforce, including certifications, courses and practical skills assessments
- an existence of underrepresented groups such as women, the neurodiverse, displaced migrants, people with disabilities
- a collaboration between industry and academia which could be intensified

Another source of relevant information on the differences between European wide activities in Cybersecurity Education is ENISA publication Towards a Common ECSC Roadmap[15]. Specifically, this publication indicates that when organizing a European wide activity, the importance of the individual objectives of each country should be taken into consideration. In this context, difficulties may arise in terms of measuring, monitoring, analysis, and evaluation of results of training activities directed at a European level but implemented and adapted at a national level. These difficulties are further exaggerated when no guidance or preferred governance model is provided for the implementation of the activities at a country level. Another conclusion that can be reached from the ENISA publication, is that funding is a challenge and the "one size fits all budget" does not apply. Different implementations of the same notion, taking into consideration the different maturity of the audience and the participation objectives, may lead to significantly greater costs and different sourcing models and collaborations.

Finally, it is relevant to mention in this context the Deloitte Study The changing faces of cybersecurity Closing the cyber risk gap[16] looking into cyber risk gaps with special attention to future technology

[15] https://www.enisa.europa.eu/publications/towards-a-common-ecsc-roadmap
[16] https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/risk/ca-cyber-talent-campaign-report-pov-aoda-en.PDF

trends and issues, specifically on the cyber risk in a data-driven distributed, machine-enabled world. The Deloitte study flags that although positive progress in business, academia, and government has been made, nevertheless, current efforts are likely not sufficient to address the cyber talent shortage effectively. The evolving technology and associated cyber risks overpass the organizations' capability to adapt. The changes in talent requirements due to evolving technologies makes the recruitment process challenging as the current talent framework lacks the human-centric approach and an outlook featuring stable groupings of talent (focused on enduring capabilities over ephemeral skills).

Consolidating all this information, we extracted a high-level graphic, depicting the challenges to the Governance of Cybersecurity Education at a European level grouped based on their common elements.


European challenges
access
cybersecurity is gender biased
cybersecurity is not understood by non-security individuals
low accessibility of the field by the broader audience
skills gap
scarcity of skilled workforce at EU level
unbalance between the offer and demand of skills between countries
different level of cybersecurity preparedness
cooperation
lack of European coordination and cooperation
lack of stakeholders cooperation
competences
need for a new, human-centric, cyber talent framework
need to understand and plan for changing talent requirements based on the evolving technology
culture
lack of cybersecurity culture
low level of societal interest in cybersecurity
sharing
difficult to understand and see the training big picture
solutions
lack of scalable and flexible solutions
lack of common certification schemes
lack of recommendations / methods and guidance on practical skills assessments
guidance
lack of governance model for the implementation of suggested activities
lack of guidance on funding
limited coordination - limited ways to scale up initiatives
heterogeneity of competencies related terminology
lack of comprehensive skills framework

2.2. Challenges at National level

ENISA has been supporting the EU Member States since 2012 in the development, implementation, and evaluation of their National Cyber Security Strategies (NCSS). Since 2017, all EU Member States have published their own NCSS. ENISA NCSS interactive map[17] (Fig.2.) lists the 20 main/common objectives of the national strategies and provides details on the status of their implementation in 31 countries (EU + UK + EFTA countries).

Fig. 2. ENISA NCSS map – Top Objectives

In view of addressing the Education related challenges, a specific objective was foreseen, namely "Strengthen training and educational programmes". At the time of closing the report, most of the Member States (27) defined their Education related strategies (Fig.3.). As seen in the Fig.2., the Education related objective is displayed as one of the top ones in terms of adoption, confirming again the importance and urgency of its implementation.

The Education objective as defined in the ENISA NCSS Good Practice Guide - Designing and Implementing National Cyber Security Strategies[18] looks into:

- Enhancing the operational capabilities of the existing information security workforce.
- Encouraging students to join and then prepare them to enter the cyber security field.
- Promoting and encouraging the relations between information security academic environments and the information security industry.
- Aligning cybersecurity training with business needs.

On the other hand, only 5 countries included in their NCSSs the Objective "Set a clear governance structure": Cyprus, Czech Republic, Greece, Ireland, and Slovakia. This objective was introduced in NCSS at a later stage, hence the low number of countries having it defined to date. Yet, this is of high importance, in the Education field included, since the governance framework defines the roles, responsibilities and accountability of all relevant stakeholders. Besides, it provides a framework for dialogue and coordination between various activities undertaken in the lifecycle of the strategy at national level, and at EU and international level.

[17] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map

[18] https://www.enisa.europa.eu/publications/ncss-good-practice-guide

Country	Strategy status	Implementation date	Objective
Austria	Complete	22/12/2021	Strengthen training and educational programmes
Belgium	Complete	20/05/2021	Strengthen training and educational programmes
Bulgaria	Complete	18/07/2016	Strengthen training and educational programmes
Cyprus	Complete	03/12/2020	Strengthen training and educational programmes
Cyprus	Complete	03/12/2020	Set a clear governance structure
Czech Republic	Complete	18/03/2021	Strengthen training and educational programmes
Czech Republic	Complete	18/03/2021	Set a clear governance structure
Denmark	Complete	01/12/2021	Strengthen training and educational programmes
Estonia	Complete	05/09/2019	Strengthen training and educational programmes
Finland	Complete	24/01/2013	Strengthen training and educational programmes
France	Complete	10/10/2015	Strengthen training and educational programmes
Greece	Complete	07/12/2020	Strengthen training and educational programmes
Greece	Complete	07/12/2020	Set a clear governance structure
Hungary	Complete	21/03/2018	Strengthen training and educational programmes
Ireland	Complete	27/12/2019	Strengthen training and educational programmes
Ireland	Complete	27/12/2019	Set a clear governance structure
Italy	Complete	27/05/2022	Strengthen training and educational programmes
Latvia	Complete	17/09/2019	Strengthen training and educational programmes
Lithuania	Complete	13/08/2018	Strengthen training and educational programmes
Luxembourg	Complete	11/10/2021	Strengthen training and educational programmes
Malta	Complete	26/09/2016	Strengthen training and educational programmes
Netherlands	Complete	21/04/2018	Strengthen training and educational programmes
Norway	Complete	31/01/2019	Strengthen training and educational programmes
Poland	Complete	31/10/2019	Strengthen training and educational programmes
Portugal	Complete	06/06/2019	Strengthen training and educational programmes
Romania	Complete	30/12/2021	Strengthen training and educational programmes
Slovakia	Complete	07/01/2021	Set a clear governance structure
Slovakia	Complete	07/01/2021	Strengthen training and educational programmes
Slovenia	Complete	01/02/2016	Strengthen training and educational programmes
Spain	Complete	01/04/2019	Strengthen training and educational programmes
Switzerland	Complete	18/04/2018	Strengthen training and educational programmes
United Kingdom	Complete	29/11/2016	Strengthen training and educational programmes

Fig. 3. ENISA – Status of Objectives implementation by Member States

The Cyberwiser EU funded project collected and displayed on their website (Fig. 4.)details about the Cybersecurity Education related objectives from all EU Member States having included this objective in their strategies - accessible via the Cyberwiser map[19]. The Education and Training in National strategies elements span between Education curricula in schools and higher education institutions, and multilingual platforms to foster a cybersecurity culture at all levels within the society, to encourage public-private partnerships, boosting the capacities of the SMEs in the area, specialized clusters of experts for enhancing the collaboration at national level, and registers of professionals to boost the cybersecurity marketplace.

[19] https://www.cyberwiser.eu/cartography

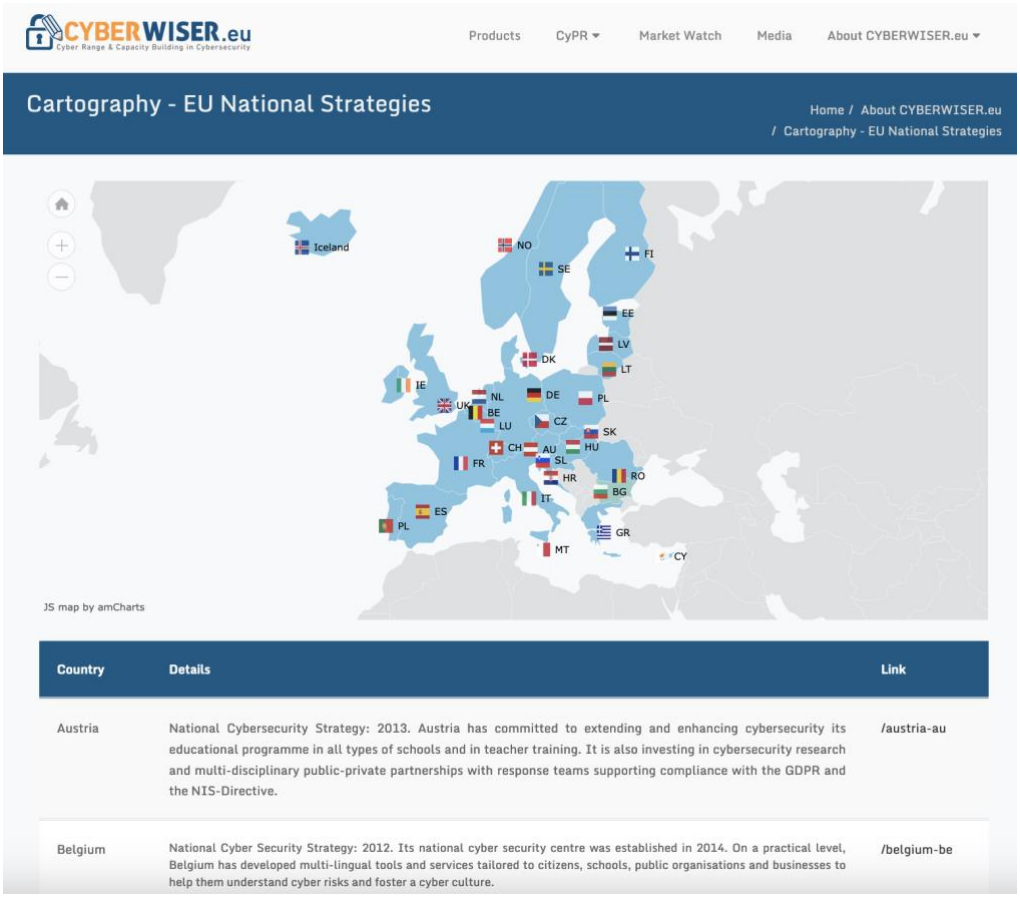


Fig. 4. Cyberwiser.eu Cartography on EU National Strategies

Zooming out, Global Cyber Security Capacity Centre undertook in 2014 a global collaborative exercise to develop the first iteration of the Cybersecurity Capacity Maturity Model for Nations (CMM), working alongside experts from academia, international and regional organisations as well as the private sector. The goal was to gather and synthesise the community's knowledge, identifying the most important factors for a nation's cybersecurity capacity and the steps necessary for the nation to reach consequent levels of maturity.

In 2021 The Cybersecurity Capacity Maturity Model for Nations (CMM)[20] was revised to address the changing threat landscape and the corresponding cybersecurity practices. This model "helps nations understand what works, what does not work and why, across all areas of cybersecurity capacity. This is important so that governments and enterprises can adopt policies and make investments that have the potential to significantly enhance safety and security in cyberspace, while also respecting human rights, such as privacy and freedom of expression." The CMM covers five Dimensions of the National Cybersecurity Capacity: (D1) Developing Cybersecurity Policy and Strategy, (D2) Encouraging responsible cybersecurity culture within society, (D3) Building cybersecurity knowledge and capabilities, (D4) Creating effective legal and regulatory frameworks, and (D5) Controlling risks through standards and Technologies. The Dimension (D3) relevant for our analysis, reviews the availability, quality, and uptake of programmes for various groups of stakeholders, including the government, private sector and the population as a whole, and relates to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes. More specifically, the Aspects Initiatives by Government, Initiative by Civil Society,

[20] https://gcscc.ox.ac.uk/cmm-2021-edition

Administration, Provision if read cumulatively describe a possible governance structure for Cybersecurity Education and training.

As indicated by the publication on the impact and adoption of the CMM, almost 100 reviews of over 60 nations have taken place (12 of these of nations in the European continent) - see Fig. 5[21]. Unfortunately, the detailed results of these reviews are not publicly available, but the general consensus is that nations are supported in their strategic actions through the CMM and incorporate corrective actions in their future strategies. Especially within the Cybersecurity Education domain, the lessons learned indicate that there is a "Disconnect between educational offerings and industry needs"[22] while the overall results indicate a "lack of cooperation and information-sharing; resources; data collection challenges".

Fig. 5. Cybersecurity capacity maturity model reviews around the world

While efforts on coordination of the activities are made on different levels, a broader coordination at European level would be beneficial. This aspect was identified as one of the needs the European ecosystem is facing in different fora and studies as previously mentioned, as well as in the report issued by ENISA under the title Cybersecurity Education Initiatives in the EU Member States[23]. The report presents an overview of the Member States' best practices when implementing cybersecurity education initiatives as well as the challenges faced by the interviewed stakeholders when carrying out the activities, with the aim to identify the needs and gaps regarding cybersecurity education and determine how ENISA can provide additional support to the Member States. Although the report targets primary and secondary schools and is limited to the ENISA mandate to support closer

[21] GLOBAL IMPACT KNOWLEDGE AND POLICY CONTRIBUTIONS FROM THE FIRST FIVE YEARS, Global Cyber Security Capacity Centre, University of Oxford. Department of Computer Science - https://gcscc.web.ox.ac.uk/sites/default/files/gcscc_booklet_web.pdf

[22] https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2018/Cyber%20drill/Session%201%20Jakob%20Bund%20-%20ITU%20Cyberdrill%202018%20%28website%29.pdf

[23] https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states?v2=1

coordination and exchange of best practices among Member States on cybersecurity awareness and education, the conclusions are also valid for the education ecosystem at large. Among the key priorities that ENISA has recommended by the experts to focus on for the EU cybersecurity roadmap, we find the following:

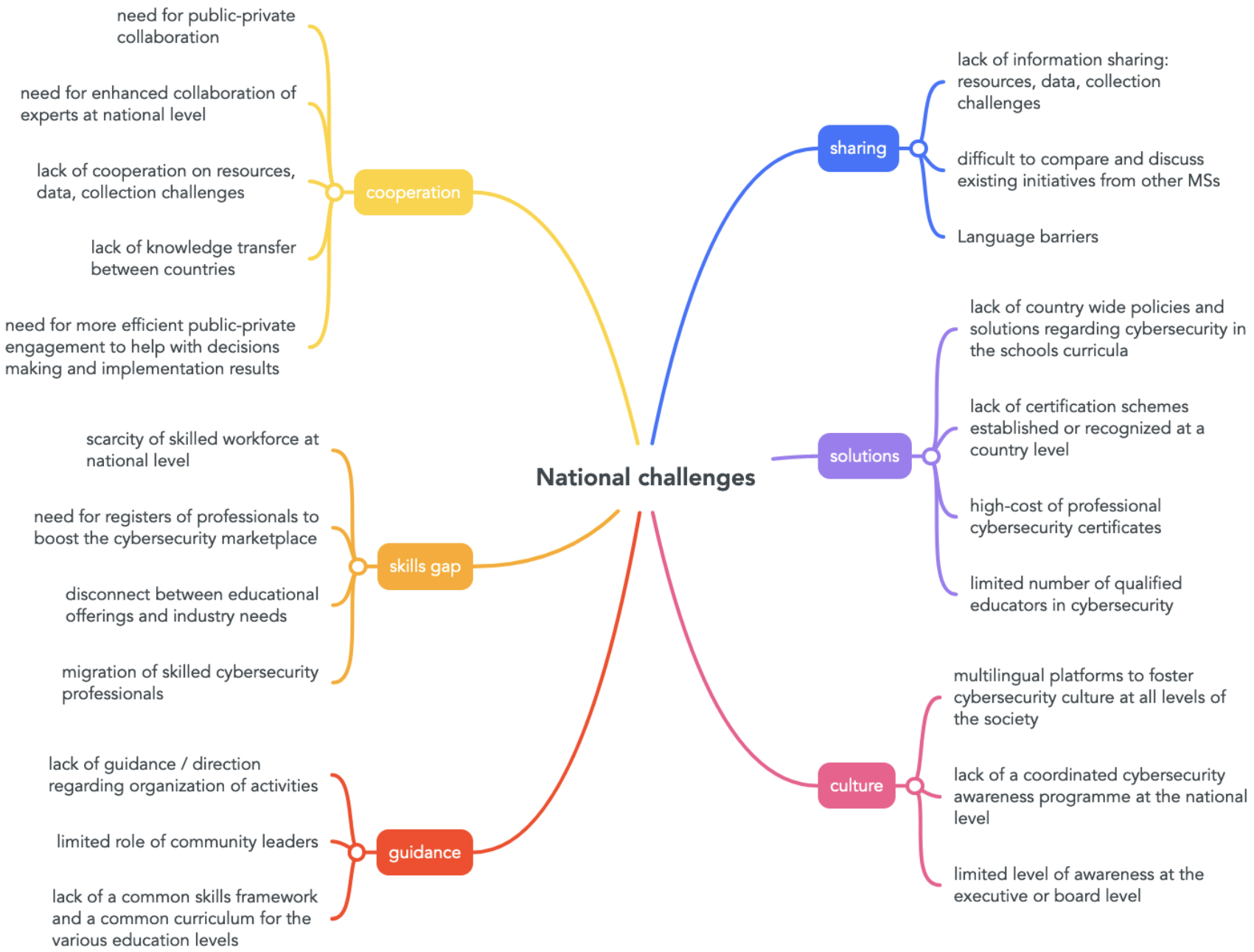
- Visibility on what the other Member States are doing: Many Member States expressed their willingness to compare and discuss existing initiatives deployed in other Member States. By doing so, the Member States would be able to learn from each other and make the most out of each State's best practices, 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 this opportunity to access more technical / operational point of views, and to build a multi-disciplinary team. Indeed, this partnership with the private sector would allow a collaborative approach around the decision-making process and implementation of cybersecurity innovation initiatives.

A study made at international level on 80 nations in 2022, and published under the title Cybersecurity education, awareness raising, and training initiatives: National level evidence-based results, challenges, and promise[24], identify a number of challenges related to cybersecurity education at a national level. As some of the countries listed in the qualitative analysis are within the European Region, we considered relevant for our review to list the challenges identified by the authors:

- under-investment in cybersecurity education especially in low-income countries
- national governments usually do not use metrics or any consistent systems to evaluate the impact of relevant policies
- discovering how to raise awareness across a broad public without instilling fear and undermining use
- inability to guide people on what to do in situations involving specific software and problems
- a lack of a coordinated cybersecurity awareness programme at the national level
- a limited level of awareness at the executive or board level
- inadequate national budgetary allocations for cybersecurity education
- a limited number of qualified educators in cybersecurity
- the migration of skilled cybersecurity professionals
- the high cost of professional cybersecurity certificates
- a lack of knowledge transfer across nations
- language barriers
- a limited role of community leaders

Consolidating all this information, we extracted a high-level graphic, depicting the challenges to the Governance of Cybersecurity Education at a National level grouped based on their common elements.

[24] https://www.sciencedirect.com/science/article/pii/S0167404822001511


National challenges
cooperation
need for public-private collaboration
need for enhanced collaboration of experts at national level
lack of cooperation on resources, data, collection challenges
lack of knowledge transfer between countries
need for more efficient public-private engagement to help with decisions making and implementation results
skills gap
scarcity of skilled workforce at national level
need for registers of professionals to boost the cybersecurity marketplace
disconnect between educational offerings and industry needs
migration of skilled cybersecurity professionals
guidance
lack of guidance / direction regarding organization of activities
limited role of community leaders
lack of a common skills framework and a common curriculum for the various education levels
sharing
lack of information sharing: resources, data, collection challenges
difficult to compare and discuss existing initiatives from other MSs
Language barriers
solutions
lack of country wide policies and solutions regarding cybersecurity in the schools curricula
lack of certification schemes established or recognized at a country level
high-cost of professional cybersecurity certificates
limited number of qualified educators in cybersecurity
culture
multilingual platforms to foster cybersecurity culture at all levels of the society
lack of a coordinated cybersecurity awareness programme at the national level
limited level of awareness at the executive or board level

2.3. Conclusions

In an attempt to identify to which extent the challenges relevant to the EU level are reflected at the national level and the other way around, we confronted them topic based (Fig. 6). It can be observed that challenges linked to skills gap, need for cooperation and sharing, and for building a cybersecurity culture are flagged both at European and at national levels. The same can be observed also with respect to existing guidance and the solutions to be put in place. On the other hand, issues linked to the enlarged competences and broad access to the field are perceived as more relevant at the European level.

	European challenges	National challenges
Skills gap	scarcity of skilled workforce at EU level unbalance between the offer and demand of skills between countries different level of cybersecurity preparedness	scarcity of skilled workforce at national level need for registers of professionals to boost the cybersecurity marketplace disconnect between educational offerings and industry needs migration of skilled cybersecurity professionals
Cooperation	lack of European coordination and cooperation lack of stakeholders cooperation	need for public-private collaboration need for enhanced collaboration of experts at national level lack of cooperation on resources, data, collection challenges lack of knowledge transfer between countries need for more efficient public-private engagement to help with decisions making and implementation results
Culture	lack of cybersecurity culture low level of societal interest in cybersecurity	multilingual platforms to foster cybersecurity culture at all levels of the society lack of a coordinated cybersecurity awareness programme at the national level limited level of awareness at the executive or board level
Guidance	lack of governance model for the implementation of suggested activities lack of guidance on funding limited coordination - limited ways to scale up initiatives heterogeneity of competencies related terminology lack of comprehensive skills framework	lack of guidance / direction regarding organization of activities limited role of community leaders lack of a common skills framework and a common curriculum for the various education levels
Solutions	lack of scalable and flexible solutions lack of common certification schemes lack of recommendations / methods and guidance on practical skills assessments	lack of country wide policies and solutions regarding cybersecurity in the schools curricula lack of certification schemes established or recognized at a country level high-cost of professional cybersecurity certificates limited number of qualified educators in cybersecurity
Sharing	difficult to understand and see the training big picture	lack of information sharing: resources, data, collection challenges difficult to compare and discuss existing initiatives from other MSs Language barriers
Competences	need for a new, human-centric, cyber talent framework need to understand and plan for changing talent requirements based on the evolving technology	
Access	cybersecurity is gender biased cybersecurity is not understood by non-security individuals low accessibility of the field by the broader audience	

Fig. 6. European and National related challenges per topics

Based on the analysis, there is a scarcity of countries wide policies in relation to cybersecurity education. In most cases, there is an objective regarding cybersecurity security education within the national cybersecurity strategy, but further analysis and incorporation in policies is not provided. Moreover, in the cases where such policies or initiatives have been carried out, there is no concrete method for the measurement of their effectiveness. This lack of measurement information is also

shown within the two REWIRE fiches publications (R5.3.1 REWIRE Fiches #1 and #2). This could be identified as a result from the insufficient European wide direction regarding such policies and initiatives.

The same overall conclusion can be reached by analyzing also other national / European challenges for instance the lack of a common cybersecurity skills framework which also aggravates national issues such as lack of sharing or collaboration. A brief analysis of some of these topics shows that they are the underlying cause for both European and National related challenges.

- The **cybersecurity skills gap** - The skills gap is manifested at a national level by the scarcity of skilled professionals to fill cybersecurity positions in general but also to man relevant education related positions. Especially the latter, leads to a difficulty to develop and deliver high-quality cybersecurity education programs, which in turn leads to a disconnect between educational offerings and industry needs, exaggerating the cybersecurity skills gap.At a European level, there is no predefined curriculum or other instrument that could be used as a basis for the development, collaboration and recognition of cybersecurity education programs. The scarcity of skilled professionals and educators, in this case is the aggregated result of the situation at a national level (with a difference of contribution from each country depending on the national conditions).
- The **lack of cooperation** - The lack of cooperation is manifested at a national level through the disconnect often observed between educational offerings and industry needs as well as through the limited ability and impact of the nationally implemented activities. Cooperations between entities can provide resources (in the form of funds but also in the form of experienced professionals), can provide useful insights on the requirements as well as an increase in the impact and effectiveness of the relevant actions. The lack of relevant guidance at a European level for such subjects lead to decreased coordination and collaboration among stakeholders, including educators, industry, and policymakers. Also, this can lead to duplication of efforts, gaps in cybersecurity education provision, and a lack of coherence in cybersecurity education policy and practice. At a European level, cooperation is equally important in order to provide direction, methodologies, case studies and other initiatives highlighting the potential, importance and ability of cooperation and partnerships between entities. Initiatives and other activities utilizing more than one entity have the ability to gain a larger audience and adoption. The lack of a common framework, methodologies, case studies and tools, do not allow for a fast adoption and implementation of such actions, minimizing the relevant risks and capitalizing on opportunities.
- The **lack of solutions** - within the context of this document and related to cybersecurity, with the term solutions we refer to certification schemes, assessment and exercising platforms, training programs at various levels etc. The lack of solutions, especially ones that are endorsed, promoted and recognized at a European level increases the cybersecurity skills gap and creates obstacles to the free movement of cybersecurity professionals across countries. There are countries (as indicated also within the European Challenges related to the skills gap) with different levels of offer and demand in terms of skills, professionals and education and training opportunities. The lack of a common framework and comparable / interoperable and recognized solutions, decreases the ability of reaching an equilibrium at a European level. Furthermore, since such solutions require knowledge and adequate funding to be developed, many countries have restricted or no access to them, further aggravating the skills gap and encouraging the migration of national professionals.
- The **lack of competencies** - Definitions regarding cybersecurity skills and knowledge (not only for the “apparent” cybersecurity roles (e.g. 12 roles of the ECSF)) and how they could be

incorporated within the various business roles are missing[25]. Cybersecurity should be incorporated into the culture and frame of mind of professionals. Currently, there is limited guidance on how this could be done in both national and European levels. The adoption of the ECSF, is a first step, but further evolution of the framework is needed, to become a truly useful, efficient and adaptable tool for the next generation of any professional. Further to that, the ECSF needs to be updated based on the advances of technology, the new and emerging risks, the evolutions in the different professions and others. Different industries and their requirements should be incorporated, and an enriched taxonomy should be created and continuously evolve over time. In the end the ECSF should be a collection of skills and knowledge to be used by every industry for any perceived role since cybersecurity should be everyone's concern.

To conclude, as stated in the beginning of the document, to derive solutions for cybersecurity education, the situation should not be looked at either only from a European or a National perspective but rather it should be addressed from a perspective of a symbiotic ecosystem with components of both levels. Hence, the governance model of the European Education ecosystem would need to bring together relevant actors at all levels addressing the challenges at European level while considering their impact and limitations at national level.

[25] For example, the ECSF includes the Cyber Incident Responder, but it does not provide guidance or tools on which skills and knowledge is needed by an HR professional.

3. Cybersecurity related governance models

In an attempt to identify different best practices fitting the cybersecurity specific ecosystem, we looked into different collaboration models, at national, European and international level. We considered it important to be aware of the different models as they will help adapt the European governance model to the national and international realities.

In line with its strategic objectives, the European Agency for Cybersecurity (ENISA), supports the efforts of the Member States with respect to their National Cybersecurity Strategies (NCSS) between others by empowering and engaging Member States through community building, by maintaining an experts' group on NCSS, and by fostering cooperation and exchange of good practices between Member States. Publications on effective collaborative models for Public Private Partnerships (PPPs) and Information Sharing and Analysis Centers (ISACs) are good examples of such effort.

3.1. The national cybersecurity Public Private Partnership (PPP) in Europe – ENISA model

Back in 2017, ENISA conducted an analysis of the existing PPP models across Europe[26] (Fig.7).

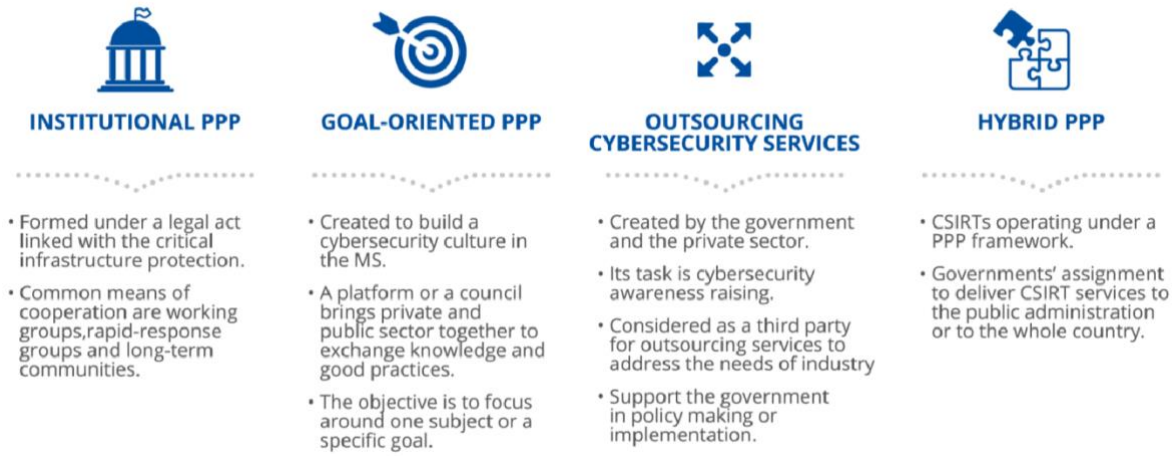


Fig. 7. Existing PPP models across Europe

While looking into the experiences of the different countries in running PPPs, the authors of the report flagged that building trust between public-private, private-private, and public-public entities has been considered as one of the biggest challenges of PPP; eventually maintaining the same level of trust seems more challenging. Besides, it was mentioned that culture is one of the most important determinants of the way private-public partnerships are being established, developed and work. There is no universal scenario of how to create a successful PPP; what works perfectly in one country can be tricky and challenging in another. That is mainly because of the cultural differences and the fact that the general relation between public and private sector differs amongst member states. In some countries formality is the most important part of PPP, while in others pragmatism is more important. Following the analysis of these models, one suggestion offered by the authors was that the public sector organizations should consider the successful strategy used by many PPP, by starting with a top-down approach and over time growing the PPP from the bottom up, so it is managed more by the private sector members.

[26] https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models

As such, for example, the European Cybersecurity Organisation (ECSO) was created in 2016 as the contractual counterpart to the European Commission to implement Europe's unique Public-Private Partnership in Cybersecurity – cPPP (2016-2020). Building upon the success of the cPPP, ECSO is today the unique European cross-sectoral and independent membership organisation for cybersecurity that gathers and represents European public and private cybersecurity stakeholders and fosters their cooperation. Members of ECSO include large companies, SMEs and start-ups, research centres, universities, end-users and operators of essential services, clusters and associations, as well as the local, regional and national public administrations across the European Union Members States, the European Free Trade Association (EFTA) and H2020 Programme associated countries.

3.2. The Information Sharing and Analysis Centers (ISACs) model

Information Sharing and Analysis Centers (ISACs)[27] are non-profit organizations that provide a central resource for gathering information on cyber threats (in many cases to critical infrastructure) as well as allow two-way sharing of information between the private and the public sector about root causes, incidents, and threats, as well as sharing experience, knowledge, and analysis. In many EU Member States, ISAC or similar initiatives exist.

In parallel with the study on the existing PPPs as previously described, ENISA conducted in 2017 also a study on Information Sharing and Analysis Centers (ISACs), collating information on best practices and common approaches.[28] The study, had amongst others the objectives:

- To identify current challenges that both the private and the public sector face in the process of setting up and developing ISACs.
- To formulate and propose recommendations with the aim of enhancing the sophistication of ISACs in Europe.

In the Fig. 8. below there are depicted some of the reasons for the creation of ISACs.

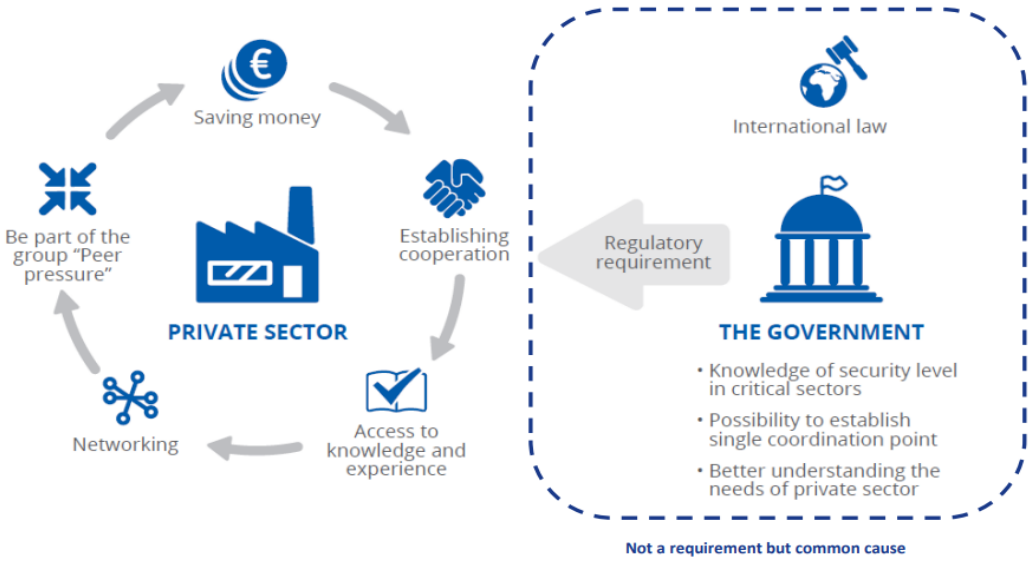


Fig. 8. Reasons for the creation of ISACs

[27] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[28] https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models

According to the study, European ISACs are focused on building partnership and trust between members. “The common challenges identified were the lack of trust between the private sector and public sector and the lack of a governance model and clear description of roles that could adhere to the needs of the group.”

The study further provides an analysis of the characteristics of different ISACs models: Country Focused, Sector Specific and International ISACs.

The International ISACs, closer to the European governance model we are exploring, bring together multi-stakeholder members from all over Europe and worldwide. Its’ features are described in the Fig. 9. below.

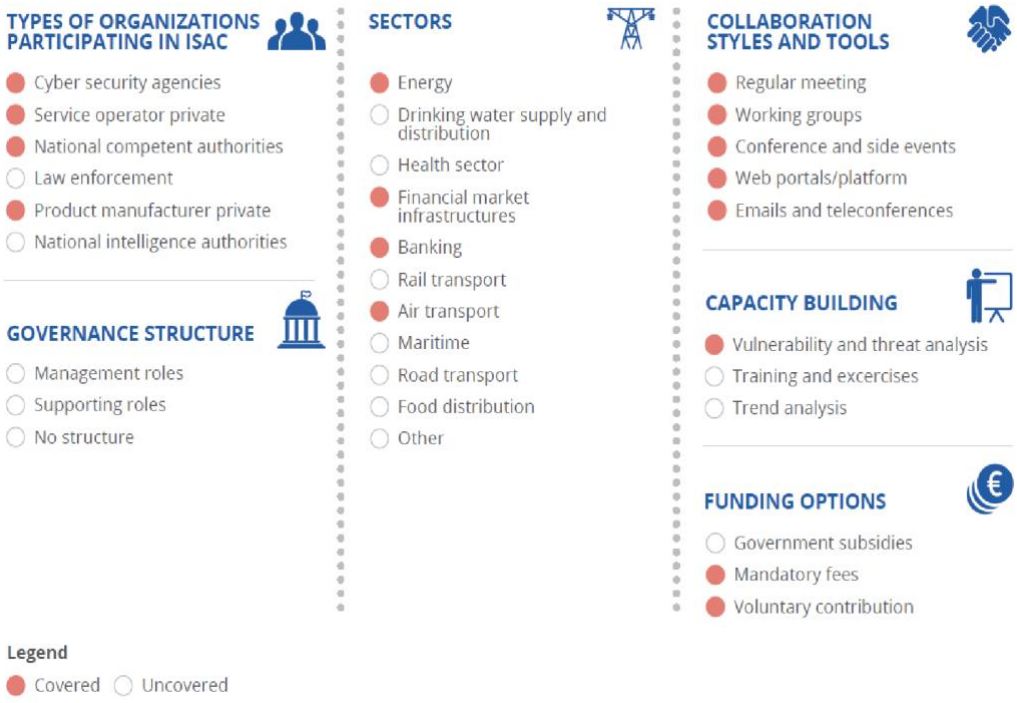


Fig. 9. Types of ISACs – International ISAC

The main challenge for this case is the fact that the process of building trust is more difficult than in the case of country-focus and sector-specific ISACs. The main reason is the cultural differences – stakeholders from different states have distinct perspective and approach to information sharing.

Between the key conclusions of the different ISACs models we consider relevant for our analysis are:

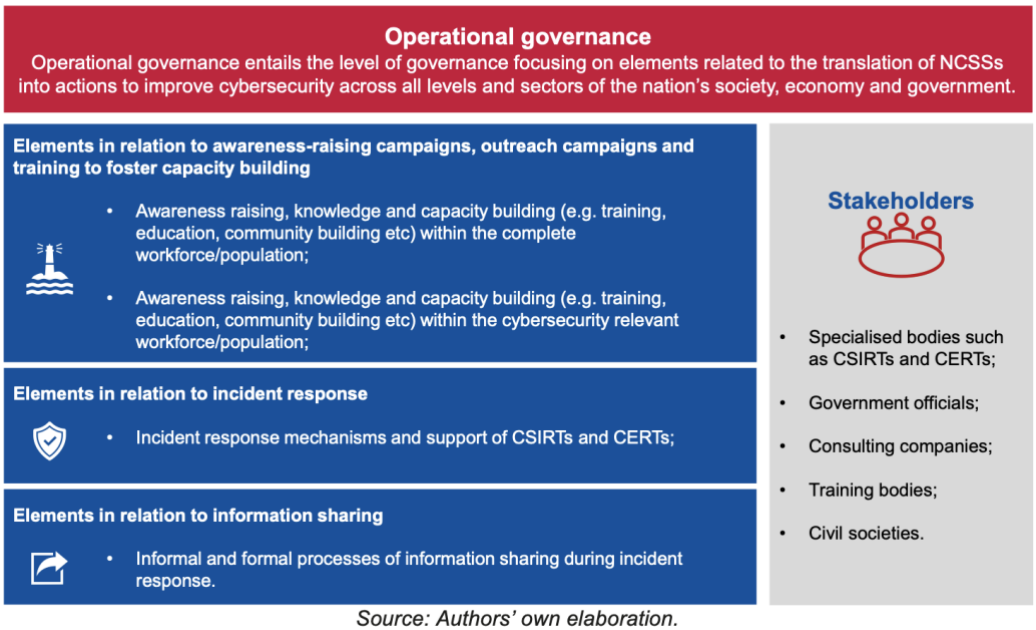
- participants (private and public sector) need to invest on trust to ensure the right level of information sharing;
- the ISACs should have a structure which motivates the private sector;
- the ISACs participants should make sure that the structure engages the public sector;
- the governance structure should include the role of a facilitator;
- ISACs should ensure funding mechanisms from their initiation;

3.3. Implementing National Security Strategies in Europe – the ENISA Framework

In February 2023 ENISA published the study on "Building Effective Governance Frameworks for the Implementation of National Cybersecurity Strategies"[29]. In view of supporting and promoting the development, deployment, and implementation of the National Cybersecurity Strategies (NCSSs) and accompanying governance models, ENISA analyses in the study existing governance models, share a set of good practices when developing a governance model and put in place the different governance elements. The study is looking into the governance model at a national level and identifies two main patterns of defining governance models as predominant, one focusing on the different layers of governance and one targeting the stakeholders and objectives of the model. As the author mentioned, an advantage of the latter is that overarching and transversal activities can be integrated, analysed, and evaluated. However, this might come at the expense of the accuracy of the definition of the roles and responsibilities of the stakeholders involved and their accountability. The study continues by defining governance models along different levels or layers. This is considered as allowing the provision of a more granular assessment of governance models. The study identifies 4 main levels of governance as predominant, that were developed further in order to build the governance framework:

a) Political governance;
b) Strategic governance;
c) Operational governance;
d) Technical governance.

In this structure, Education is mainly covered in the Operational Governance model:



Source: Authors' own elaboration.

Fig. 10. ENISA - Operational Governance Model Example

The report makes an important point on the monitoring of the effectiveness and the successful deployment of the governance models. Good practices in the context of establishing monitoring

[29] Building Effective Governance Frameworks for The Implementation of National Cybersecurity Strategies, European Union Agency for Cybersecurity, February 2023, ISBN: 978-92-9204-604-0

mechanisms have been identified from the Member States part of this report, such as extended KPIs and a platform that would enable the exchange of the progress. A set of existing KPIs are listed as options to be adopted (re-used) at the national level.

For the purpose of our endeavor the EU Cybersecurity index (work in progress within ENISA) looks to be the most appropriate one as the EU Cybersecurity Index aims at helping Member States making informed decisions by providing insights on the cybersecurity maturity and posture of the Union and MS policies, capabilities and operations.

3.4. The OECD Education governance model

Back in 2016, the OECD Centre for Educational Research ran the project Governing Complex Education Systems (GCES) looking into which models of governance are effective in complex education systems and which knowledge systems are needed to support them. The GCES project has defined three themes considered vital for effective governance of modern education systems: accountability, capacity building and strategic thinking. These challenges were addressed in the paper Governing Education in a Complex World[30] while also exploring some educational models from Austria, UK, the Netherlands and the United States. Between the main findings of the analysis, relevant to our purpose we could list:

- effective governance works through building capacity, open dialogue, and stakeholders involvement
- the national or state level remains very important in triggering and steering education reforms, even in decentralized systems
- there is a need to develop key principles for system governance (not just agreement on where to go, but how to get there)

The paper concludes with a list of elements (Fig. 11.) for effective governance that keep the focus on the process, allow systems to adapt and respond to complexity, and build on dialogue and participation of multiple actors.

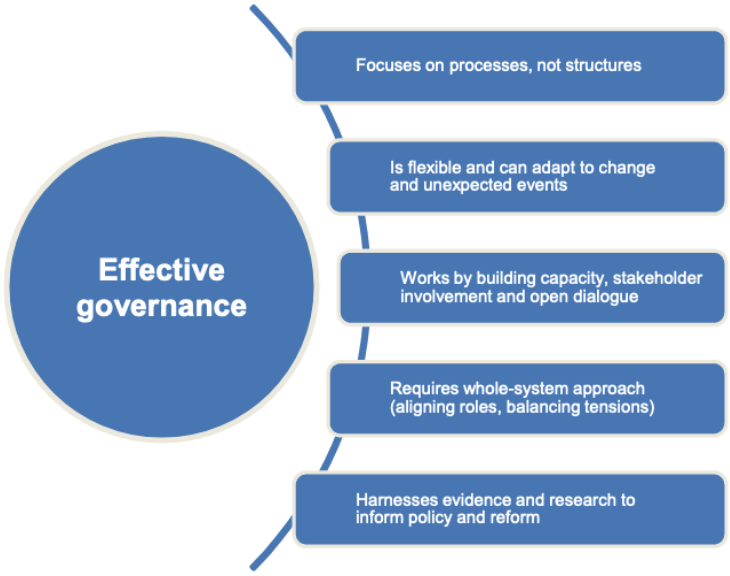


Fig. 11. OECD - Governing Complex Education Systems, Elements of effective governance model

[30] https://read.oecd-ilibrary.org/education/governing-education-in-a-complex-world_9789264255364-en#page1

As part of the same GCES project, the analysis of approaches to reform and governance in complex education systems goes further by running six in-depth case studies on a variety of OECD countries, those results were documented in the paper Education Governance in Action - Lessons from Case Studies[31]. Following the analysis of the case studies, as a way forward towards building / reforming complex systems such as education, the authors presented the concept of Trust. "There are four broad strategies for building, restoring and sustaining trust in a complex education system: stakeholders' engagement, accountability, capacity building and strategic thinking". The different countries' examples regarding the Factors for trust breakdown, Policies to rebuild trust and Policies to sustain trust long-term are captured in Fig. 12 below.

	Stakeholder engagement	Accountability	Capacity building	Strategic thinking
Factors for trust breakdown	– Lack of consultations – Uncertainty about consequences	– Lack of accountability – Lack of transparency	– Insufficient capacity to implement reforms	– Lack of long-term thinking
Policies to rebuild trust	– (Formal and informal) consultations with variety of stakeholders about consequences of reform	– External evaluation and review – Ownership among stakeholders	– Greater autonomy of teachers, school leaders – Building capacity of stakeholders (e.g. training of evaluators)	– Stepwise implementation of reforms; piloting – School management council
Policies to sustain trust long-term	– Regular consultations with stakeholders	– External evaluation and review – Financial resources - funding	– Professionalisation of teachers; higher teachers' remuneration – No earmarking of education-specific funds	– National council for long-term strategy – National educational agreement between ministry and stakeholders

Fig. 12. OECD Education Governance in Action - Lessons from Case Studies, Mapping of countries examples

3.5. The USA NICE community model

In the USA, there is a federal level approach for education and training in cybersecurity with the aim to present the topic to the widest possible audience. It aims at bringing cybersecurity awareness to the community, by following public-private partnership principles. The National Initiative for Cybersecurity Education (NICE) Community[32] groups together all the relevant actors of the ecosystem from Academia, Industry and the Government (see Fig.13.)

Within the NICE Community there is a strong emphasis on public and private partnership to develop concepts, design strategies and pursue actions for cybersecurity education, training, and workforce development. Several resources are made available to the community for the widest possible audience, between them Database for education and training provider, and platform for users of the NICE framework to interact and share experiences and best practices.

[31] https://read.oecd-ilibrary.org/education/education-governance-in-action_9789264262829-en#page1

[32] https://www.nist.gov/itl/applied-cybersecurity/nice/community

Credit: NICE

Fig. 13. The NICE Community model

As modus operandi, the NICE Community Coordinating Council is comprised of three Working Groups (Modernize Talent Management; Promote Career Discovery; Transform Learning Process) and four Community of Interest groups (Apprentices in Cybersecurity; Cybersecurity Skills Competitions; K12 Cybersecurity Education; NICE framework). Each subgroup meets independent of the NICE Community and reports out at the NICE Community Meetings.

3.6. European Cybersecurity Competence Centre and Network Community

The European Cybersecurity Competence Centre (ECCC) aims to increase Europe's cybersecurity capacities and competitiveness, working together with a Network of National Coordination Centres (NCCs) to build a strong cybersecurity Community. The community is defined in the Regulation setting up the ECCC[33] and it is seen as contributing to the mission of the Competence Centre and the Network, and enhancing, sharing and disseminating cybersecurity expertise across the Union. The current document lists the types of organisations eligible to be part of the community and the domains they should come from, between them "training and education". Furthermore, a clear process is put in place with respect to the registration of an actor to the Community, strictly via the NCCs, of working – in (domains related) working groups, and of reporting - through the Strategic Advisory Group, towards the Executive Director and the Governing Board.

3.7. Main takeaways

A summary of the main takeaways of the chapter is presented below:
EU PPP model:

- Trust between the actors of the partnership is an ongoing process
- Culture determines how a PPP should be established and work.
- Setup a PPP top down and over time manage it bottom up.
- the structure is self sustainable, based on membership fees and not necessarily dependent of any specific project funding
- structure is organized in Workgroups having a consensus approach to guidelines

ISACs model:

- The lack of trust between the private sector and public sector challenges the sector.
- The lack of a governance model and clear description of roles that could adhere to the needs of the group makes the collaboration difficult.

[33] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021R0887&from=EN#d1e1214-1-1

- The process of building trust at international level is more difficult than in the case of country-focus and sector-specific formations because of the cultural differences impacting the stakeholders' perspective and approach to information sharing.
- The community should have a structure which motivates the private sector.
- The community participants should make sure that the structure engages the public sector.
- The governance structure should include the role of a facilitator.
- The community should ensure funding mechanisms from their initiation as a group.

NCC model:

- A governance model focusing on the different layers of governance allows the provision of a more granular assessment of individual levels.
- A governance model targeting the stakeholders and the objectives allows transversal activities to be integrated, analysed, and evaluated. However, this might come at the expense of the accuracy of the definition of the roles and responsibilities of the stakeholders involved and their accountability.
- Monitoring the activities based on clear KPIs is important; Exchanging information on clear and measurable indicators and associated good practices would help with running tailored conversations based on the priorities of the different groups involved.

OECD model:

- Effective governance works through building capacity, open dialogue, and stakeholders involvement.
- The national or state level remains very important in triggering and steering education reforms, even in decentralized systems.
- There is a need to develop key principles for system governance (not just agreement on where to go, but how to get there).
- Trust between stakeholders is paramount in complex education systems.
- The strategies for Building, Restoring and Sustaining trust in a complex education system: stakeholders' engagement, accountability, capacity building and strategic thinking.

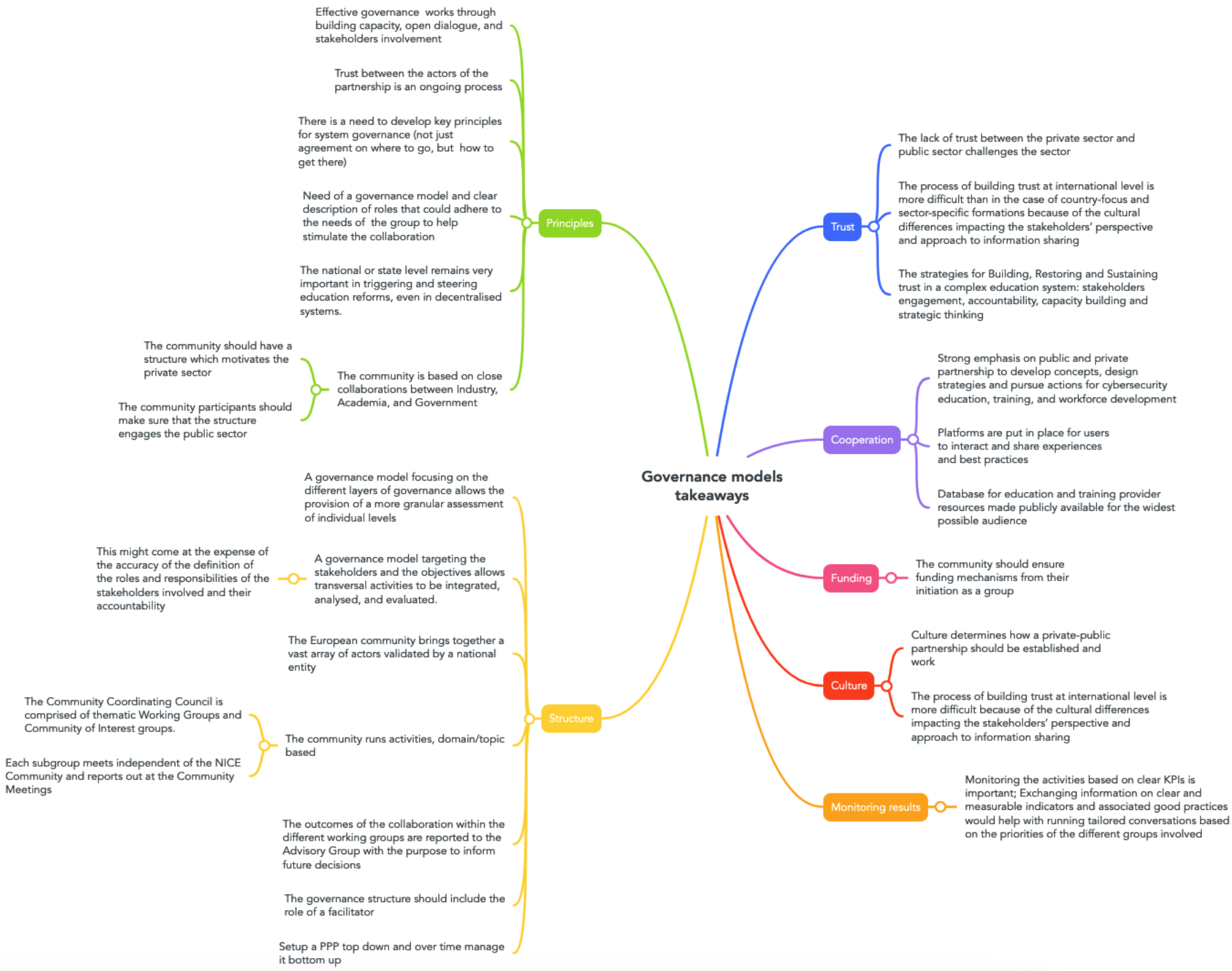
NICE Community model:

- Strong emphasis on public and private partnership to develop concepts, design strategies and pursue actions for cybersecurity education, training, and workforce development.
- The community is based on close collaborations between Industry, Academia, and Government.
- Platforms are put in place for users to interact and share experiences and best practices (e.g, on the NICE framework).
- Database for education and training provider resources made publicly available for the widest possible audience.
- The Community Coordinating Council is comprised of thematic Working Groups and Community of Interest groups. Each subgroup meets independent of the NICE Community and reports out at the Community Meetings.

ECCC Community model:

- The European community brings together a vast array of actors validated by a national entity.
- The community runs activities, domain/topic based.
- The outcomes of the collaboration within the different working groups are reported to the Advisory Group with the purpose to inform future decisions.

There is no surprise to see that, although coming from the different European or international models of governance, the different observations converge. For the purpose of our endeavor, we clustered them as shown below. This exercise will later materialize in identifying the characteristics of the governance model.


Governance models takeaways
Principles
Effective governance works through building capacity, open dialogue, and stakeholders involvement
Trust between the actors of the partnership is an ongoing process
There is a need to develop key principles for system governance (not just agreement on where to go, but how to get there)
Need of a governance model and clear description of roles that could adhere to the needs of the group to help stimulate the collaboration
The national or state level remains very important in triggering and steering education reforms, even in decentralised systems.
The community is based on close collaborations between Industry, Academia, and Government
The community should have a structure which motivates the private sector
The community participants should make sure that the structure engages the public sector
Trust
The lack of trust between the private sector and public sector challenges the sector
The process of building trust at international level is more difficult than in the case of country-focus and sector-specific formations because of the cultural differences impacting the stakeholders' perspective and approach to information sharing
The strategies for Building, Restoring and Sustaining trust in a complex education system: stakeholders engagement, accountability, capacity building and strategic thinking
Cooperation
Strong emphasis on public and private partnership to develop concepts, design strategies and pursue actions for cybersecurity education, training, and workforce development
Platforms are put in place for users to interact and share experiences and best practices
Database for education and training provider resources made publicly available for the widest possible audience
Funding
The community should ensure funding mechanisms from their initiation as a group
Culture
Culture determines how a private-public partnership should be established and work
The process of building trust at international level is more difficult because of the cultural differences impacting the stakeholders' perspective and approach to information sharing
Monitoring results
Monitoring the activities based on clear KPIs is important; Exchanging information on clear and measurable indicators and associated good practices would help with running tailored conversations based on the priorities of the different groups involved
Structure
A governance model focusing on the different layers of governance allows the provision of a more granular assessment of individual levels
A governance model targeting the stakeholders and the objectives allows transversal activities to be integrated, analysed, and evaluated.
This might come at the expense of the accuracy of the definition of the roles and responsibilities of the stakeholders involved and their accountability
The European community brings together a vast array of actors validated by a national entity
The community runs activities, domain/topic based
The Community Coordinating Council is comprised of thematic Working Groups and Community of Interest groups.
Each subgroup meets independent of the NICE Community and reports out at the Community Meetings
The outcomes of the collaboration within the different working groups are reported to the Advisory Group with the purpose to inform future decisions
The governance structure should include the role of a facilitator
Setup a PPP top down and over time manage it bottom up

4. The CONCORDIA governance models

4.1. The CONCORDIA stakeholders' groups

A key objective for CONCORDIA was to inclusively and comprehensively engage diverse competencies/ stakeholders to build an EU-wide Cybersecurity ecosystem. Recognizing that different stakeholders have different interests, and represent different levels of competencies, CONCORDIA defined 3 types of stakeholders' groups and setup dedicated processes to engage with them:

A. The National Cybersecurity Coordination Centres and Agencies Stakeholders Group (NSG);
B. The Liaison Stakeholders Group (LSG);
C. The Observer Stakeholders Group (OSG).

Since cybersecurity is multidimensional where various domains and associated stakeholders interplay and need to be identified, CONCORDIA made the distinction between four main domains for collaboration:

- Sovereignty, CERT & NIS
- Economic Development & Competition
- Research & Innovation
- Education & Skills.

Topics that are part of these domains were seen as to be addressed by all 3 stakeholders' groups from their specific perspective. For instance, the NSG approach was more general since their approach was more at strategy and governance level. On the other hands the OSG being more technical, built around "interests" derived from the domain, as listed in the registration form[34].

Each of the stakeholders' groups, were seen as performing three main tasks, based on the mission to help build a platform for trustworthy exchange of ideas, approaches, topics of joint actions and collaborations:

1. Build and maintain a trusted zone of dialogue and collaboration: sharing, develop and sustain good practices and other information regarding the various objectives of the Cybersecurity Competence Community, the network, and the public Cybersecurity Atlas, including without limitation mapping common state of play and state of the art and addressing relevant gaps;
2. Discuss how to coordinate, operationalize and sustain the various domains set forth above, including addressing both the numerous engagements as well as preconditions, also with the aim to add to the actual functioning of the Cybersecurity Competence Community of which the respective liaisons may, or will become part of;
3. Cooperate in the field of cybersecurity innovation, research, economic and societal implications encouraging cross-borders and other collaboratives programs, projects and event-driven developments.

An overview of the 3 CONCORDIA stakeholders' groups is presented in Fig. 14 below.

[34] https://www.concordia-h2020.eu/observers-stakeholder-group-osg-registration/

	National Cybersecurity Competence Centers and Agencies Stakeholders Group (NSG)	Observer Stakeholders Group (OSG)	Liaisons Stakeholders Group (LSG)
Role type	Awareness & Coordination	Observe & Coordinate	Liaison
Type of actors	national governmental bodies; national-level cybersecurity center	standardization and certification bodies; education actors; corporate, research organizations; cybersecurity related EU organizations	large organization inside and outside EU
Purpose	interconnect the National Cybersecurity Competence Centers and Agencies (NCCCA) in the EU Member States	support the development of the proposed network (including both the National Cybersecurity Coordination Centers and Cybersecurity Competence Community)	engage European institutions such as the European Union Agency for Cybersecurity (ENISA), European Defence Agency (EDA), Europol, or European Central Bank (ECB) for coordinated coverage across such European agencies
Focus	technical, policy, and governance issues	topics specific issues	policy and governance issues

Fig. 14. Summary of the 3 CONCORDIA Stakeholders' Groups

It is essential to note the differences with already established stakeholders' groups in Europe. Some aim to build cybersecurity (ECSO working groups, FIC Observatory[35]), some promote operational cooperation (CSIRTs network), and some others facilitate the exchange of information on specific domains (NLO network[36], the ENISA Advisory Group, and SCCG4[37]). Other cybersecurity pilots include stakeholders to receive feedback from them on the cybersecurity roadmap and to provide them a preview of products and services (SPARTA friends[38] and associates and ECHO participants[39]). However, the three CONCORDIA stakeholders' groups setup in 2020 mimic the structure proposed that time by the European Commission for the European Cybersecurity Competence Center and Network to detect the challenges and functionalities of such a structure.

4.2. The CCN Education focus group and beyond

Beginning of the year 2020 CONCORDIA Task 3.4 initiated a collaboration with the other 3 pilot projects ECHO, SPARTA and CyberSec4Europe and built the Cybersecurity Competence Network CCN-Education focus group. The aim of the group was to take advantage of the strengths of each pilot project, combining and consolidating the available resources and investing them in complimentary

[35] https://observatoire-fic.com/en/dna/
[36] https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office
[37] https://ec.europa.eu/digital-single-market/en/stakeholder-cybersecurity-certification-group/
[38] https://www.sparta.eu/partners/
[39] https://echonetwork.eu/join-echo/echo-participants/

activities that converge to a common goal. In this process Task 3.4 invited to assist and provide guidance both the EC DG CONNECT and ENISA representatives in order to ensure that our work is aligned to the policy developments. Starting 2021 the European organization ECSO was also actively involved in the group work by exchanging on the results and cross-promoting initiatives.

The pilots' representatives originated mainly from academia but also from certification organisations and business network organisations and were based in different EU countries. Although over the 3 years of collaboration individuals participating in the groups changed, the pilots' main representatives were unchanged and constituted the core of the focus group. At the beginning of each year, together with ENISA, the group determined the themes of prime concern for the period, based on an analysis of the individual projects' priorities. In view of taking this decision on the group priorities, we have attached to each of the topics a maturity of collaboration level using the scale: undefined / limited/ progressing / mature / optimizing. The main topics for collaboration over a year were selected from the categories 'progressing' and 'mature' while those under the heading 'optimizing' were used for communication purposes.

This model will be further exploited within the European Cybersecurity COmmunity ECCO project[40] commissioned by the ECCC end of the year 2022 to support activities needed to develop, promote, coordinate and organise the work of the Cybersecurity Competence Community at European Level, within the scope and operations of the ECCC and NCC Network. The ECCO project is led by ECSO and brings within the consortium 13 cybersecurity stakeholders from the public and private sector. Importantly, representatives of all the 4 pilot projects CONCORDIA, SPARTA, ECHO and CyberSec4Europe are part of the consortium, thus ensuring the legacy of the pilots' outcomes and communities. More specifically ECCO is structured in three main tasks: (Task A) is mainly focused on the mapping and analysis of the European Cybersecurity Competence Community; (Task B) targets the stimulation and collaboration within the European Cybersecurity Community; (Task C) works towards linking the European Cybersecurity Competence Community with the ECCC and the NCCs network. Regarding the support of the community for education, training, and gender balance, the ECCO Task B.6 main objectives include the design of a strategy with specific tasks including the mapping of the educational offer in the EU, the analysis of the main curricula, and the standardization of the professional training in cybersecurity. This goal aims to be achieved with the collaboration of the NCCs, ENISA, industry, and educational institutions. In this way, ECCO will enhance the availability of educational standards, upgrade, and update professionals' skills over time, giving additional attention to female professionals, by stimulating collaboration within the community and contributing to the development of subcommunities including that of the educators, trainers', cyber range experts'; students' and Women4Cyber.

[40] https://cybersecurity-centre.europa.eu/news/european-cybersecurity-competence-centre-and-network-new-eu-funded-project-support-cyber-community-2022-12-20_en

5. A Governance model for the European Education Ecosystem for Cybersecurity

5.1. Mapping the actors

Extrapolating from the CONCORDIA roadmap concepts, in order to understand how to build and sustain a trusted, hybrid interconnected Ecosystem of Ecosystems, we should be focusing on two notions: knowing and understanding the ecosystem and communities, beyond the more formal structures, and exploring how to team up, share and act.

In an attempt to understand the dynamic of the European cybersecurity education ecosystem we propose mapping the actors based on level of influence and roles

With respect to the level of influence, within CONCORDIA governance model for the Education ecosystem we are considering the following:

- **Local**: organisations acting at city level or having an impact on a group of cities/region within the same country
- **National**: organisations acting at EU Member States level
- **EU**: organisations acting at European Union level or having an impact on a group of EU Member States

When it comes to the roles, within CONCORDIA governance model for the Education ecosystem we are considering the following:

- **Regulator**: organisation having the mission to regulate an area of activity for the public good, such as the European Commission, Certification bodies, National ministries
- **Aggregator**: organisation that pull together a set of resources (monetary and non-monetary) for the use of a community, such as ENISA, ECCC, Associations
- **Coordinator**: organisation empowered to harmonize the usage of a set of resources for the purpose of reaching specific Education related objective
- **Influencer**: organisation/ individual having the capacity to affect the course of an action, such as NGOs, think-tanks, but also companies
- **Provider**: organisation/ individual offering to the market Education related services, such as Universities, research organisations, training and solution providers, corporates
- **Beneficiary**: organisation / group/ individual capitalizing on the Educational offer, such as students, professionals, small and big companies

It is to be noted that one actor of the Education ecosystem could play multiple roles and could have a level of influence on more than one level. Links to the specific organisations included in the structure below are referred to in the Annex of this document.

Level of influence			Entity	Role					
EU	National	Local		Regulator	Aggregator	Coordinator	Influencer	Provider	Beneficiary
			European Parliament (EP)						
			European Council						
			Council of the European Union						
			European Data Protection Board (EDPB)						
			European Union Agency for Cybersecurity (ENISA)						
			European Centre for the Development of Vocational Training (CEDEFOP)						
			European Cybersecurity Competence Centre (ECCC)						
			The Computer Emergency Response Team (CERT-EU)						
			The Network and Information Systems (NIS) Cooperation Group						
			Certification bodies						
			European School of Administration (EAS)						
			European Personnel Selection Office (EPSO)						
			European Commission (EC)						
			Associations (ECSO..)						
			Think-tanks, NGOs						
			European Education organisations (EITD..)						
			Formal education (system / provider)						
			Cyber Incident Response Teamn (CSIRTs)						
			Governments and Ministries of Education						
			Higher education institutes						
			Industry						
			Research organizations						
			Students and students' organisations						
			Educators and educator's organisations						
			Syndicates						
			Vocational education and training (VET) providers						
			National Cybersecurity Coordination Centres (NCCC)						
			Training / solutions providers						
			Community						
			Individuals						

5.2. Objectives

Following the analysis done in Chapter 2 on the challenges of the cybersecurity education ecosystems at national level superposed on those at European level, CONCORDIA proposes a set of Overarching Objectives (OO) to be tackled by the ecosystem. These objectives are covering different challenges and are suggested to be used to support the discussions within the ecosystem. It is on the ecosystem actors to agree on the importance of the proposed objectives and their level of urgency.

OO1: Establish sharing resources and information models - addressing challenges described under the categories Cooperation, Sharing and Solutions

OO2: Strengthen the cybersecurity workforce - addressing challenges linked to the Skills Gap, Guidance and Competences

OO3: Build a European cybersecurity culture - addressing challenges linked to Culture and Access

5.3. Characteristics of the governance model

Given the different considerations mentioned in the previous chapters in terms of heterogeneity of the ecosystem as a whole and on different levels, of national priorities and European objectives, this paper does not aim at proposing a concrete governance model of the European cybersecurity education ecosystem but rather at describing the most important principles and characteristics such a model should have. In doing so, we are building on the elements identified when analyzing different governance models subject of Chapter 3 and based on the CONCORDIA consortium experience described in Chapter 4.

Characteristics of the proposed model:

- **Agile** – an agile governance approach means not only efficient collaboration between the actors involved in the process of managing existing problems but also implies a forward-looking approach with the view of anticipating problems before they materialize.
- **Inclusive** – a multi-stakeholder collaboration bringing together all the actors of the ecosystem would help with anticipate potential risks and opportunities.
- **Trust based** – sharing information under specific agreements, and best practices would contribute to increasing the body knowledge which could be further used as a basis for new policies for the benefit of the ecosystem.
- **Smart sovereignty** – this approach is needed to help balance international cooperation with national autonomy. It should consider a multimodal approach, covering national, regional and EU level specificities. This way, national policies could better integrate multilateral considerations as they are developed, potentially enabling leaders to balance national demands with the benefits of European coordination. On the other hand, at European level, it will make room for a better understanding of cultural differences, thus helping to tailor the policies accordingly.
- **Multimodal** - covering national, regional and EU level specifics – the model should not focus on the EU level observation of national developments as all realistic work is done in education and training institutions. Thus, EU level governance can be more focused on collection of tools, best practice to be shared on national level as well as to construct the national level nodes by providing the proper platform for cooperation. National level should focus on implementation of recommendations provided as well as organization of local activities and coordination with other national nodes.

- **Flexible** – refers to the ease of accessing and taking part in different groups' activities and interactions of specific actors without being formally obliged to be validated by a specific entity; this flexibility would apply mainly to sharing/registering information on open platforms. It would complement the "inclusive" approach by ensuring that all actors interested to contribute with information would have an easy way to proceed.
- **Sustainable** - The governance model should promote sustainability in all aspects of the education ecosystem. This includes promoting sustainable practices in education delivery, ensuring the sustainability of the education infrastructure and resources, and ensuring the long-term viability of the education ecosystem itself, at all levels, establishing sustainable funding mechanisms and meeting the evolving needs of learners and society as a whole. The model should be sustainable in the long term, for all parties involved (training organizations, prospective trainees, employers, policy makers, …).
- **Impact focused** - The governance model should place a strong emphasis on measurement and monitoring to ensure that the EU education ecosystem is meeting its objectives effectively and efficiently. This includes monitoring the performance of learners, educational institutions, and education programs to identify areas for improvement and opportunities for synergies. The governance model should ensure that the results of measurement and monitoring are transparently communicated to stakeholders, including learners, educators, policymakers, and the public. This will help to build trust and confidence in the education ecosystem.
- **Methodological sound** - by applying recognized monitoring, analytical, coordination and co-creation tools. Those tools are to be well thought through beforehand and the complete set to be developed, from monitoring (indicators and process), analytical (indicators based and management, like SRL, MRL, Benchmarking) to coordination (setting process, alignment of national processes etc.).

5.4. Interaction between the actors of the ecosystem

The characteristics mentioned above aim to further support and guide the cybersecurity ecosystem actors from a European to a local level. There is evidence from the challenges identified within Chapter 2 of this document, that communication between all actors and direction is needed in cybersecurity education. The relationship between the actors of the cybersecurity ecosystem should be seen as synergistic / symbiotic. The approach proposed is intended to give a voice to all actors of the ecosystem and build only one platform for communication, the EEEC platform.

As such,

In terms of **information exchange**, and considering the different interests of the actors of the Education ecosystem, a way forward could be split into the following two main categories:

- **Policy talks** - bringing together representatives of Regulators, Aggregators and Influencers at the EU and National level.
- **Operational talks** - bringing together Coordinators, Providers and Beneficiaries at EU and National level.

These talks would be organised with a predefined frequency (e.g., once per year for policy talks and twice a year for operational talks), will have a pre-set agenda built around the 3 overarching objectives (OO) and would be chaired by representatives of EU countries on a rotational basis. The outcomes of the Operational talks would be brought in the Political talks to help better shape different EU policies for the benefit of the EU cybersecurity ecosystem at large. Besides, since the model proposed suggests involving as many stakeholders as possible from all role-categories and all levels, the input from the

stakeholders would be collected via the EEEC platform, country base, and in all EU languages. This approach would ensure inclusiveness of all interested actors but would require a dedicated person/organisation per country to ensure the moderation of the national section, translate and cluster the different input in preparation for the Policy and Operational talks.

In terms of **coordination and guidance** a way forward could be split into some concrete activities. The activities suggested below[41] are directly linked to one of more of the Overarching Objectives (OO1-3) and would benefit from the exchanges between the actors of the ecosystem during the policy/operational talks.

- **Pilot /model projects** - Creating model projects that would allow the testing of collaboration and partnership models. The results of such pilots would then be provided as tools / templates to be further used by the relevant actors at different levels.
- **European wide activities** - European wide activities, especially ones that are focused on the identification of the needs of the population should be designed. Such activities could be surveys on the levels of skills of different audiences per country within the European Union, assessments on the maturity of the cybersecurity education mechanisms per country within the European Union and others. These activities should be planned at a European level, executed at national levels and the results should be shared between all levels. [42]
- **The European Cybersecurity Skills Framework** (ECSF) - The ECSF should have a specific owner. ENISA with the advice and aid of the Ad-Hoc Working Group on the European Cybersecurity Skills Framework, developed the ECSF in 2022. The Ad-Hoc Working Group on the European Cybersecurity Skills Framework (2023-2025) will assist ENISA in the governance, implementation, and future evolution of the ECSF, although the full scope of the support and activities have not been clarified. It is imperative though, that the governance activities for the sustainable maintenance and evolution of the ECSF are identified and assigned, to ensure the effective operation of this tool.
- **A Cybersecurity Book of Knowledge**[43] - A baseline body of knowledge needs to be created, adopted, and mapped to the various knowledge identified within the ECSF. This body of knowledge should be created and an entity which should make sure it remains current, is updated based on results of the market and other activities and is evolved over time.

5.5. Funding

The kick-start of the collaboration within the EU ecosystem would initially require EU funding. These could be directed, for instance, towards setting up the platform for communication and sharing, for running an EU wide targeted communication campaign to make the initiative known and attract the stakeholders to the initiative, for organizing local events where needed. On the other hand, the moderation of the national sections of the platform would be covered with National funding. Yet, the activity of the group will be impact focused, with clear and measurable objectives, and the structure is meant to be sustainable in the long term. As such, partners in this endeavor would see the value-for-money and would decide to fund, lead, and support components of the governance model. On the other hand, the activities regarding coordination and guidance should be coordinated by the ECCC and then be propagated to the NCCCs for adoption or implementation.

[41] The activities will be further expanded in the context of REWIRE project

[42] An example of such activity is the DESI index - https://digital-strategy.ec.europa.eu/en/policies/desi

[43] Examples of such documents are: WG5 PAPER European Cybersecurity Education and Professional Training: Minimum Reference Curriculum SWG 5.2 I Education & Professional Training November 2022 (version 3.0) and UK Cybok - https://www.cybok.org/ataglance/

5.6. Measuring the impact

In order to measure the impact of the EEEC collaboration, specific indicators, both at EU and National level would be needed to be adopted. One option would be to build on the EU Cybersecurity index (work in progress within ENISA) which aims at helping Member States making informed decisions by providing insights on the cybersecurity maturity and posture of the Union and Member States policies, capabilities, and operations. As such, the Education related composite indicator would look into determining the cybersecurity skills preparedness of each EU country. The indicator would measure the country's progress on different cybersecurity education dimensions, would help in exchanging best practices within the Operational talks, and advance discussions towards tailoring/developing specific policies within the Policy talks.

Annex: Links to Stakeholders organizations at EU level

European Parliament (EP)
https://www.europarl.europa.eu/portal/en

European Council
https://www.consilium.europa.eu/en/european-council/

Council of the European Union
https://www.consilium.europa.eu/en/

European Commission (EC)
https://commission.europa.eu/index_en

European Data Protection Board (EDPB)
https://edpb.europa.eu/edpb_en

European Union Agency for Cybersecurity (ENISA)
https://www.enisa.europa.eu/

European Centre for the Development of Vocational Training (CEDEFOP)
https://www.cedefop.europa.eu/en

European Cybersecurity Competence Centre (ECCC)
https://cybersecurity-centre.europa.eu/index_en

The Computer Emergency Response Team (CERT-EU)
https://cert.europa.eu/

The Network and Information Systems (NIS) Cooperation Group
https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

European School of Administration (EAS)
https://europa.eu/eas/index_en.htm

European Personnel Selection Office (EPSO)
https://epso.europa.eu/en