together against cybercrime

TaC

# THE HUMAN FACE OF CYBERSECURITY

## YOUTH STANDS FOR CYBERSECURITY SKILLS

Youth IGF

Active since 2011

## CONTACT

Youth IGF Movement

Email: youthigf@youthigf.com

## DISCLAIMER

The views expressed in this report do not necessarily reflect the official positions of the Microsoft Corporation, nor of TaC International.

**OCTOBER 2020**

## Acknowledgements

The present report was prepared as part of a joint effort by the Youth IGF Movement[1], administered by TaC International[2] with the support of the Microsoft Corporation.

This report is based on a number of public consultation debates and interviews carried out by the Youth IGF Movement in July 2020[3].

The report will be presented and discussed during the Cybersecurity Month[4] in October 2020 and at the Virtual UN IGF 2020[5].

[1] Referred to in this report as the Youth IGF. The Youth IGF was created in 2011 during the MAG IGF meeting. More information is available at: www.youthigf.com
[2] www.againstcybercrime.org
[3] Accessible at: https://www.facebook.com/pg/globalyouthigf/videos
[4] Learn about the Cybersecurity month at : https://cybersecuritymonth.eu
[5] www.intgovforum.org

Youth IGF
Active since 2011

## Young people recommend POLICY ACTION

**Promote** and encourage media literacy on cybersecurity at the EU level.

**Establish** and promote a common EU cybersecurity skills curricular guidance or a recommendation for guidance on cybersecurity skills curricula for different formal education levels that can be recommended to the member states.

**Support** existing volunteering actions for the young at the end of their studies and encourage the development of new ones within EU institutions working on cybersecurity, like Cybersecurity EU volunteers. This can also be done as an upskilling mechanism, to help the young gain their first experience in the field and to promote learning by doing.

**Call** for a common EU certification for cybersecurity skills training modules (e.g. under one of the priorities of the digital skills agenda, in collaboration with ENISA).

**Better** public-private-youth dialogues on cybersecurity topics in the EU context.

Youth IGF
Active since 2011

## Young people recommend DEVELOPMENT ACTION

**Promote upskilling initiatives** recognised by the industry that will focus on cross-sectoral cyber skills.

**Facilitate the development of a set of guidelines** for employers on ensuring descriptions of cybersecurity job offers are up-to-date and written in language comprehensible for entry-level professionals, HR departments and cybersecurity departments.

**Facilitate and encourage the development of** learning concepts for teaching cybersecurity skills to pupils (of different age groups).

**Facilitate the development of the recommendation** for better internal communication (or intra-departments) on cybersecurity skills for industry.

**Improve the dialogue** in between EU institutions and the young on cybersecurity by initiating an annual (physical/or virtual) meeting and through initiatives such as the Youth IGF.

## TABLE OF CONTENTS

## YOUTH IGF AND CYBERSECURITY

The Youth IGF,[6] created in 2011, is a recognised initiative, described by the United Nations Internet Governance Forum (www.intgovforum.org) as an existing IGF Initiative.

The Youth IGF is a global movement that operates as a multi-stakeholder network. It allows the young (18-35 years) to discuss and take a lead in issues related to internet governance. A number of countries are implementing targeted projects either locally or nationally. These activities are organised by the young on a volunteer basis based on the methodology provided by the Youth IGF.
The Youth IGF is based on the principles of the UN Internet Governance Forum (IGF) and has full respect for them.

The Youth IGF has inspired youth activism on internet governance all over the world, resulting in the creation of several Youth IGF Chapters across the globe. Youth IGF Ambassadors have become recognised digital policy leaders in a number of countries.

---

The Youth IGF engagement on cybersecurity is based on the Paris Call for Trust and Security in Cyberspace[7]. It is also a response to the Christchurch Call,[8] which emphasises the importance of working with civil society to promote community-led efforts for a free, open and secure internet, as well as the UN Secretary-General's Roadmap for Digital Cooperation,[9] which identifies trust and security in the digital environment as one of its eight key areas for action.

The Paris Call, made during the 2018 Internet Governance Forum, underlines the importance of peace in cyberspace and of guaranteeing online security for citizens. It welcomes *"collaboration among governments, the private sector and civil society to create new cybersecurity standards that enable infrastructures and organizations to improve cyber protections."*

The development and implementation of new cybersecurity standards go hand in hand with the cybersecurity skills that will be essential to guarantee cyber protection for citizens. For this reason, the Youth IGF aims to ensure that young professionals are active in the field of cybersecurity skills and develop recommendations for action based on the voice of the young to help narrow the cybersecurity skills gap. A lack of cybersecurity professionals could make the implementation of the Paris Call problematic, meaning there is today an urgent need for multi-stakeholder action on cybersecurity skills.

[6] The movement is administered by an international NGO, TaC-Together against Cybercrime International. TaC International is both non-profit and neutral. The movement is financed through a multi-stakeholder funding scheme and contributions from donors. TaC International has a separate budget dedicated to the activities of Youth IGF.
TaC – Together against Cybercrime International is a non-profit anti-cybercrime organisation based in France (founded in 2009) with its headquarters in Geneva and in Paris. TaC operates internationally.
[7] https://pariscall.international/en/
[8] https://www.christchurchcall.com
[9] https://www.un.org/en/content/digital-cooperation-roadmap/

# BACKGROUND AND PURPOSE

The aim of this assessment is to explore how we can improve and innovate cybersecurity education and training for young professionals by using informal education options, in order to foster the improvement of cybersecurity skills by doing and learning at the same time.

A new way of approaching cybersecurity skills will create better opportunities for the younger generations in term of professional development, social utility and participation in the digital transformation of societies. The main goal of our project is to create better opportunities for the young in the cybersecurity area by helping to eliminate the cybersecurity skills gap.

This paper is based on the following methodology:

1. Assess the existing educational situation at EU level focused on a general EU approach towards cybersecurity skills;

2. Assess the needs and innovative ideas of young professionals and activists during a consultation period related to cybersecurity skills;

3. Carry out an analysis of the two parts of the assessment and propose tangible recommendations for action at EU level.

**Three main points will be addressed by the paper:**

• A consolidated EU response to the lack of cybersecurity skills

The idea is examine existing insufficiencies in the cybersecurity skills educational process (and also to take a look at what happened during the COVID-19 crisis) in the EU (general view) and to analyse the potential benefit of a consolidated EU response to the identified insufficiencies.

• Better mobility/innovation and exchange of best practices; a better approach to solving gaps in cybersecurity skills curricula

The idea is to take a look at the potential benefits of a consolidated EU response to the lack of cybersecurity skills in terms of better mobility, more robust knowledge-based skills, and better exchange of innovative approaches and best practices.

• These skills will answer current and future market demand. We will avoid a situation in which the young are surplus to market requirements (e.g. in possession of a technical diploma but unable to find employment).

Here we would like to take a look at the benefits of the general approach to cybersecurity skills in the EU in terms of market demand and professional skills efficiency if developed at EU level.

# INTRODUCTION

The majority of cybersecurity strategies around the world underline the lack of skills. However, in many cases these national and supranational strategies, such as the European Union's Cybersecurity Strategy, focus on training events or the lack of skills on legislation for lawmakers or IT aspects.

At a time of unprecedented sanitary crisis in all countries around the world, the lockdown situation has made cyberspace a vulnerable environment for online threats (phishing, malware, ransomware attacks, online fraud, the use of cash mules, etc.) commonly referred to as cyber-criminal threats, as pointed out by Europol on 27 March.

All spheres of life are now dependent on cyberspace. Professionals and organisations are exposed to cyber risk even more than before the virus reached our societies. Remote workers are not always prepared, and companies have been forced to introduce online or remote solutions in a rush, without always having the appropriate online security procedures in place.

The lack of a coherent, consolidated answer from the EU in the face of the increased cyber risk is ultimately related to the lack of cybersecurity skills among professionals in the private and public sectors. This may be due to the fact that cybersecurity professionals have encountered situations that they have never experienced or faced in real life before, such as the assault on critical health infrastructure, especially that belonging to small or medium-size health organisations, which we have seen during the COVID-19 outbreak.

The difficulties in finding an appropriate and swift response once a cybersecurity issue has been discovered is potentially related to the lack of real professional skills gained at operational level, including cross-sectoral cooperation and the lack of public-private cooperation in cybersecurity skills educational curricula. The role of private sector actors and corporations active in the cybersecurity field is important for robust and coherent cybersecurity skills curricula, since they can deliver experience at operational level that is of vital use for future professionals.

## I. CURRENT SITUATION

Over the last few decades there has been much discussion of the lack of professionals in the cybersecurity field in the EU, and many organisations and corporations often speak about the cybersecurity skills gap[10].

There is no clear definition of what is meant by cybersecurity skills, and each professional field tries to give its own definition. The tendency is to relate cybersecurity skills to computer skills, even if cybersecurity skills do not just require technical or computer skills, but rather a complex spectrum of different skills, of which computer skills form a solid part. However, the issue of the cybersecurity skills gap may be directly related to an understanding of what cybersecurity skills represent today or what they should represent today[11].

Today, the understanding of cybersecurity skills in the EU is influenced by the bloc's main policy and regulatory mechanisms on cybersecurity. These policies are essential, as they shape the general environment and create a suitable educational space for cybersecurity professionals.

### 1. Political will

We would like to see what kind of recommendations/policies and calls for action on fostering European cybersecurity skills exist[12] at EU level.

*EU Cybersecurity Strategy*

**➔ The EU has a rich legal and policy landscape on cybersecurity. The European Union's Cybersecurity Strategy[13] has been in force since 2013.**

Under the paragraph on "Raising awareness"[14] in the Cybersecurity Strategy, it reads:

*"The Commission asks ENISA to:*
*• Propose in 2013 a roadmap for a "Network and Information Security driving licence" as a voluntary certification programme to promote enhanced skills and competence of IT professionals (e.g. website administrators)."*

We can see that ENISA, the European Union Agency for Cybersecurity, here plays a central role in enhancing the skills of cybersecurity professionals. The text doesn't identify what kind of IT skills need to be reinforced and concerns only IT professionals, so people who are already active in cybersecurity work are classified as having an IT background.

This obviously leaves behind all other cybersecurity professionals who are not identified as being IT cybersecurity professionals.

[10] https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/cybersecurity-talent-gap.html
[11] At the time of drafting of this report, July 2020.
[12] At the time of publication of this report, July 2020.
[13] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001
[14] p.8 of the EU Cybersecurity Strategy

In terms of training, the Cybersecurity Strategy identifies several points:

1) *"The Commission invites the Member States21 to: (…)*
*• Step up national efforts on NIS education and training, by introducing:*
*training on NIS in schools by 2014; training on NIS and secure software development and personal data protection for computer science students; and NIS basic training for staff working in public administrations."*[15]

We see that the strategy clearly encourages the member states to introduce education on information system security to schools' curricula, however there is no indication of the skills that need to be part of the curricula. The second paragraph and the whole text give us an indication that the text has in mind computer or IT skills.

2) *"The Commission asks the European Police College (CEPOL) in cooperation with Europol to:*
*• Coordinate the design and planning of training courses to equip law enforcement the knowledge and expertise to effectively tackle cybercrime."*[16]

Here the text gives a clear indication that specific training for law enforcement needs to be developed. So the paragraph concerns a very specific subset of cybersecurity professionals.

3) *"The Commission asks Eurojust to:*
*• Identify the main obstacles to judicial cooperation on cybercrime investigations and to coordination between Member States and with third countries and support the investigation and prosecution of cybercrime both at the operational and strategic level as well as training activities in the field."*[17]

Here the text encourages the development of training courses, mainly for better investigation and prosecution of cybercrime.

4) *"The High Representative will focus on the following key activities and invite the Member States and the European Defence Agency to collaborate:*
*• Assess operational EU cyberdefence requirements and promote the development of EU cyberdefence capabilities and technologies to address all aspects of capability development - including doctrine, leadership, organisation, personnel, training, technology, infrastructure, logistics and interoperability;"*[18]

Here we see that the text speaks about the development of cyberdefence training, once again intended for professionals, that is people with a professional presence in a particular field of cybersecurity: cyberdefence.

*5) "Utilise different EU aid instruments for cybersecurity capacity building, including assisting the training of law enforcement, judicial and technical personnel to address cyber threats; as well as supporting the creation of relevant national policies, strategies and institutions in third*

[15] p. 8 of the EU Cybersecurity Strategy. NIS is the Network and Information System Security (NIS) Directive.
[16] p. 11 of the EU Cybersecurity Strategy.
[17] Ibid.
[18] Ibid.

*countries;"*[19]

The text once again underlines the need for training for specific categories of professionals working on cybersecurity.

*6) "Coordination and collaboration will be encouraged among ENISA, Europol/EC3 and EDA in a number of areas where they are jointly involved, notably in terms of trends analysis, risk assessment, training and sharing of best practices. They should collaborate while preserving their specificities. These agencies together with CERT-EU, the Commission and the Member States should support the development of a trusted community of technical and policy experts in this field."*[20]

It is interesting to note that the text encourages cooperation between different EU agencies working on cybersecurity from different angles. It doesn't mention education or skills, but we can probably surmise that the "development of a trusted community" also includes upselling methods and targeted capacity-building initiatives. However the text is silent about the definition of the term "development of a trusted community."

*NIS Directive*

**➔Another major document in place since 2016 in the EU is the directive concerning measures for a high common level of security for network and information systems across the Union, more commonly referred to as the NIS Directive[21]. The NIS Directive has the following to say about training needs:**

1) *"… ENISA should provide assistance in those areas that correspond to its own tasks, as set out in Regulation (EU) No 526/2013, namely analysing network and information system security strategies, supporting the organisation and running of Union exercises relating to the security of network and information systems, and exchanging information and best practice on awareness-raising and training."*[22]

The text in the above paragraph approaches indirectly the question of skills or potential training courses, in terms of "supporting the organisation and running of Union exercises." These exercises can function as an upskilling mechanism, but not necessarily.

2) *" 3. The Cooperation Group shall have the following tasks: (…)*
*(k) discussing the work undertaken with regard to exercises relating to the security of network and information systems, education programmes and training, including the work done by ENISA; (…)"*[23]

[19] p. 16 of the EU Cybersecurity Strategy.
[20] p. 18 of the EU Cybersecurity Strategy.
[21] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[22] Paragraph 38 of the NIS Directive. ENISA is the EU Agency for Cybersecurity. More information: https://www.enisa.europa.eu
[23] Article 11 of the NIS Directive.

This paragraph makes direct mention of the need for cooperation on education programmes. We can suppose that the programmes can be formal or informal education programmes that fall under the ENISA mandate.

*Cyber Diplomacy Toolbox*

**➔ Another important document that provides policy lines on cybersecurity in the EU and formulates a diplomatic response to the issue of cybersecurity is a document called Council Conclusions on Cyber Diplomacy,[24] known as the "cyber diplomacy toolbox"[25].**

The document:

"STRONGLY ENCOURAGES the EU and its Member States to:

– develop a coherent and global approach to cyber capacity building, which on one side brings together technology, policy and skills development within a broader and overreaching EU development and security agenda, and on other side facilitates the design of an effective EU model for cyber capacity building;[26], (…)

- tackle growing cyber threats and challenges by increasing resilience of critical information infrastructure and by reinforcing close cooperation and coordination among international stakeholders through initiatives such as the development of confidence building, common standards, international cyber exercises, awareness-raising, training, research and education, incident response mechanisms,"[27]

The document makes direct mention of the need for skills development and gives an indication of what kind of cybersecurity skills need to be developed. This paragraph is quite unique, since it proposes a global cross-sectoral reading of the kind of cybersecurity skills that need to be developed. At the same time, the paragraph encourages a global approach and calls for reinforced collaboration among different stakeholders in the cybersecurity field.

In conclusion, current EU cybersecurity policy and legislative documents mention the need for cybersecurity education, quite often in terms of capacity building and training. However, none of them proposes a structural reading of what kind of cybersecurity skills we need to develop[28]. The **cyber diplomacy toolbox** is a unique document that can serve as a basis for discussion on cybersecurity skills today, as it encourages a global approach and speaks directly about the need for cybersecurity skills.

[24] http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/en/pdf
[25] https://www.consilium.europa.eu/en/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/
[26] p.10 of the document.
[27] p.11 of the document.
[28] We need not to forget that cyberspace is quite changing and a non-holistic approach towards skills might quickly become outdated.

Therefore it is the right moment today to think about what kind of cybersecurity skills we need and how to avoid the appearance of a real cybersecurity gap, as noted by many industry players[29]. As MEP Marina Kaljurand has said, "what we see today after the pandemic, the pandemic has brought all digital topics much higher in the political agenda.*"*[30]

It is also the right moment because the European Union's Cybersecurity Strategy[31] and NIS Directive [32] are about to be reviewed as part of a communique called "Europe's moment: Repair and Prepare for the Next Generation", adopted on 27 May, 2020 by the EU Commission[33].

> *The present EU Commission, under the Presidency of Ursula von der Leyen, has all digital topics high in the agenda. Yes we have the NIS Directive, yes we have the Cybersecurity Strategy, but they need reviewing in today's context. In today's context we have to pay much more attention to artificial intelligence, the Internet of Things; as I mentioned, the certification of online services. ... We need to upgrade the system that we have. … And I will argue that today we are not paying enough attention to cybersecurity, we are not dedicating enough financial resources, enough human resources, because it's a race. Cybercriminals will not disappear*[34]*.*

We need also to mention that the European Union is about to develop a new Digital Services Act[35] as a part of its European Digital Strategy. The future Digital Services Act[36] will not focus on cybersecurity, but will specify rules on how to keep users safe from illegal services online and protect their fundamental rights. "With digital services, we have to look into the security of the IoT, we have to look into the security of online services, because today we do not have it," said Marina Kaljurand on 2 July, 2020[37]. Therefore, it is crucial to underline the importance of cybersecurity skills in the digital services environment.

[29] See this report by cybersecurity giant Kaspersky: https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf

[30] MEP Marina Kaljurand, interview with Youth IGF TV on 2 July, 2020, at: https://www.facebook.com/110382750596633/videos/314062422959656/?__so__=channel_tab&__rv__=all_videos_card

[31] More information at: https://ec.europa.eu/digital-single-market/en/policies/cybersecurity

[32] Public consultation is available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive

[33] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940

[34] MEP Marina Kaljurand, interview with Youth IGF TV on 2 July, 2020. Ibid.

[35] Public consultation is available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12417-Digital-Services-Act-deepening-the-Internal-Market-and-clarifying-responsibilities-for-digital-services

[36] More information at: https://ec.europa.eu/digital-single-market/en/digital-services-act-package

[37] Ibid.

## II. EU CYBERSECURITY EDUCATION GENERAL APPROACH

(…) *one of the problems we have in Europe is the mandate….the final responsibility for the education system that they will choose (…) it's not up to Europe to force this change on the education system*[38].

### 1. Formal track

Formal education is an organised educational model that is structured and systematic. We would like to get a brief overview of the existing situation in the cybersecurity field in the EU. In order to put together an effective and comprehensive picture of the existing cybersecurity skills tracks in educational curricula, we will study three different youth age bands: from school to university.

In the last 10 years we have seen the development of a general understanding that safety online needs to be taught at different levels in school. The level of understanding varies, depending on the country and national priorities. The cybersecurity curricula quite often presents a disparate picture, ranging from a structural way of teaching IT and online safety at school[39] at different levels to a simple non-mandatory school activity in which teachers or social workers raise awareness among the young of online threats[40]. This creates quite important differences among EU countries in terms of approach. "For me cybersecurity on a human level, with a human face, starts with cyberhygiene. Like we brush our teeth in the morning, how often do we do change our passwords, what are our passwords," MEP Marina Kaljurand told Youth IGF TV[41] on 2 July, 2020[42].

According to the European Commission, there is a need to create a cybersecurity education programme for primary and secondary schoolchildren[43].
In a 2017 communication,[44] the EU Commission called on all member states to include cybersecurity in their "academic and vocational training curricula."[45]

The EU Digital Education Action Plan 2018-2020[46] mentions "Cybersecurity in education" as Action 7 of the Action Plan, which is composed of 11 actions. It clearly encourages the teaching of cybersecurity issues in primary and secondary schools.
Priority 2, called: *Developing digital competences and skills* of the Commission Staff Working Document[47] on the recently announced Digital Education Action Plan 2021-2027[48] identifies as

[38] MEP Eva Kaili, interview with Youth IGF TV on 7 July, 2020, at: https://www.facebook.com/110382750596633/videos/737453287008860/?__so__=channel_tab&__rv__=all_videos_card
[39] e.g. in Estonia, as explained by the MEP Marina Kaljurand.
[40] e.g. in France with B2i and C2i,
https://eduscol.education.fr/numerique/dossier/archives/b2ic2i/@@document_whole
[41] More information at : www.youthigf.tv
[42] Ibid.
[43] https://eit.europa.eu/news-events/news/eit-digital-teach-3-000-schoolteachers-europe-about-cybersecurity
[44] JOIN 2017 (450): Joint Communication of the European Commission and European External Action Service: Resilience, Deterrence and Defence: Building strong cybersecurity for the EU.
[45] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018DC0022&from=EN
[46] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[47] https://ec.europa.eu/education/sites/education/files/document-library-docs/deap-swd-sept2020_en.pdf

next step of the priority line 7 (Cybersecurity in Education): *…a blended learning course for teachers on cybersecurity* [49], which has to be available in the second half of 2020.

*Primary education*

It is important to note that the EU Commission is about to develop a *new Digital Education Action Plan*[50] due to the recent changes ushered in by the coronavirus. This review is also part of the *A Europe Fit for the Digital Age*[51] strategy and will be part of the *New Generation EU Recovery Instrument*[52]. Open consultation[53] is ongoing to have a say on cybersecurity skills education at all levels.

It is difficult to assess the situation and the level of cybersecurity education in primary schools as in EU member states this is dependent to a large degree on national priorities and even on regional approaches within a country. It can also depend on the particular school and represent differences in terms of approach between private and public schools.

The general study on the use of ICTs in schools, including the situation with schools' digital policies, has been done by the European Commission, first in 2013[54] and then in 2019[55], following the EU Digital Education Action Plan. Deeper analysis of the aforementioned findings would need to be carried out with regard to cybersecurity education in primary schools.

What is evident is that the situation in the education at primary level in the EU member states varies from one country to another. "In Estonia we start teaching our kids cyberliteracy or cyberhygiene in the first grade, at seven years old," said MEP Marina Kaljurand.[56] In another EU country it can happen that cybersecurity education is not at all part of the school curricula in primary schools.

*Secondary education*

> *I would say, each and every educational document in each and every country should have digital skills, should have digital literacy for secondary school or school kids. … It has to start from the very beginning (…) and we also have to pay attention to girls*.[57]

The situation at secondary level is quite similar to primary level, with a better presence of courses or extra-curricular activities related to online safety. Once again, it is difficult to present

---

[48] https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[49] Ibid., p.9.
[50] https://ec.europa.eu/education/news/public-consultation-new-digital-education-action-plan_en
[51] https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age
[52] https://ec.europa.eu/commission/presscorner/detail/en/ip_20_940
[53] certification
Open until September 4, 2020 at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12453-Digital-Education-Action-Plan/public-consultation
[54] https://ec.europa.eu/digital-single-market/en/news/survey-schools-ict-education
[55] https://ec.europa.eu/digital-single-market/en/news/2nd-survey-schools-ict-education
[56] MEP Marina Kaljurand, interview to the Youth IGF TV on July 2, 2020. Ibid.
[57] Ibid.

a detailed country-specific assessment in our report as information is scant and a large-scale study needs to be done, but we can already highlight the following trends.
At secondary level we quite often find curricular or extra-curricular courses or awareness-raising sessions on online safety aimed at the young. However, even given that different initiatives exist and the level of cybersecurity education is different in all countries and relies on national priorities in this area, only a few countries have adopted a structured attitude towards cybersecurity education that gives the young a clear understanding of what cybersecurity skills are.

In conclusion, secondary schools quite often amalgamate cybersecurity skills education with the awareness-raising sessions on online safety that are accompanied in a number of schools with the opportunity of voluntary participation in coding activities.

This means that cybersecurity skills are not fully taught in schools and their educational impact is rather limited. This situation is partly influenced by the absence of EU-based common cybersecurity skills guidance (as exists in other non–EU countries[58]) and the lack of a clear understanding for teachers and social/educational workers of what constitutes cybersecurity skills.

The secondary education approach would require educational modules on cybersecurity that will present all components of cybersecurity and would open a door to the young in terms of existing professions, cybersecurity volunteer work, gaining initial experience, meeting cybersecurity professionals, discussing entry into the profession and receiving information on exiting post-secondary education. Media literacy in cybersecurity has an important role to play here.

This structured approach will allow the EU not only to foster EU-based cybersecurity skills and raise a new generation of cybersecurity professionals, but also to try to reduce the cybersecurity skills gap and therefore reinforce the EU's independence in terms of cybersecurity.

**➔ Three points to mention with regard to cybersecurity education at primary and secondary levels.**

**First,** we lack a kind of EU-based common cybersecurity skills guidance for primary and secondary schools, that is a kind of recommended cybersecurity skills curriculum for primary and secondary schools.

This lack of recommended curricular guidance quite often results in a lack of understanding among teachers and social/educational workers of what cybersecurity is about and what kind of information in terms of new skills needs to be part of the lessons that they deliver to pupils. Teachers and social/educational workers may need to develop an understanding of cybersecurity skills by themselves, based on their personal attitude towards digital and cyber issues. This demonstrates the lack of training for teachers and social/educational workers in

[58] Here in the United Sates, https://niccs.us-cert.gov/formal-education/integrating-cybersecurity-classroom

their national language in a number of EU member states on what constitutes cybersecurity skills and how to teach cybersecurity.

This brings us to another point, which is the lack of structural age-graded educational/pedagogical material on cybersecurity for children to be used by teachers and recommended for use. The existence of a general cybersecurity skills guidance could facilitate the development of these essential materials.

The **second point** is related to the first and concerns the fact that cybersecurity education is quite often concentrated only on tips related to online safety, and does not provide pupils or children with information relating to future professional cybersecurity skills, e.g. how to react if an attack happens, what instant action we should take if we become the victim of a cyber attack, how to code, etc.

This is also related to the non-existance of EU common curricular guidance on cybersecurity skills that need to be taught at primary and secondary levels, even if sporadic initiatives exist in the EU member states.

Writing for the World Economic Forum, Paul Mee, Partner and Lead for the Oliver Wyman Forum's Cybersecurity Initiative, says: "As teachers incorporate more online educational tools into their curricula and parents permit children to play with online apps, they can simultaneously teach students of all ages basic cybersecurity skills and encourage them to become cybersecurity experts themselves. Children can be equipped to protect themselves from cyberthreats automatically, just like they look both ways before crossing the street."[59]

The **third point** is strongly related to the second one.

> *Not only shall education and training be addressed, but also current and future career opportunities, as the number of students could be improved – for instance with more awareness on the availability and type of future jobs and by introducing cyber security topics no later than secondary school level (probably even before).*[60]

Our second point underlines that in EU countries pupils and secondary school students do not receive information on topics apart from online safety (in the best-case scenario) in a structured way (based on a common EU understanding of cybersecurity skills).
This therefore represents a missed opportunity to introduce them to the cybersecurity profession, as well as structured access to the information on the existing post-secondary education options that exist across the EU.

This leads to a situation in which young people don't really understand what the cybersecurity professions and jobs are and that cybersecurity nowadays is not just about IT, but is a rather more complex field. This also creates a more pronounced gender gap and reinforces

[59] https://www.weforum.org/agenda/2020/03/we-need-to-start-teaching-young-children-about-cybersecurity/
[60] https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

stereotypes related to STEM[61], as they don't have the opportunity to access accurate information about cybersecurity skills.
At a user level, they also clearly miss a number of elements that allow them to fully incorporate, develop and afterwards improve their cyberhygiene.

*University level*

A common Cybersecurity Higher Education Database[62] has been developed by ENISA, the European Cybersecurity Agency. It demonstrates the role of ENISA in cybersecurity education and underlines the importance of developing education on cybersecurity. This database lists higher education degrees in cybersecurity available in the EU, EFTA, and other European countries. It is open to academic institutions and today lists a total of 86 degrees in 19 countries. The objective is to have a one stop-shop for students, who can choose the degree best-suited to their interests. In the Database, "the term 'cybersecurity topic' refers to the topics in the knowledge areas of the Cybersecurity Curricula 2017 developed by the Joint Task Force on Cybersecurity Education (Joint Task Force on Cybersecurity Education, 2017)."[63]
The Cybersecurity Curricula for Post-Secondary Degrees developed by the U.S.-based Association for Computing Machinery is an important step in trying to provide guidelines in terms of the skills components that need to be part of the Cybersecurity degree. However, it will be important to have a set of EU Cybersecurity Curricula guidelines for post-secondary education based on EU priorities, needs and realities, and which will take into account the voice of the students.
While the academic cybersecurity landscape is quite rich today in the EU,[64] the majority of degrees are focused on IT/technical aspects of cybersecurity or legal studies[65] and only a few propose a large and complete reading of what cybersecurity represents today. Also, few produce legal specialists on cybersecurity who are able to understand the technical aspects and technical specialists/IT specialists who are able to understand policy or legal language in cybersecurity.

> *Universities have "added" a cyber security undergraduate or graduate degree to their curricula. This is often viewed as a "specialisation" or "add-on" to or just a re-branding of a Computer Science or Information Security degree. Unfortunately, many curriculum designers fail to realise the critical importance of the interdisciplinary nature of this area.*[66]

This cross-sectoral skills knowledge is crucial as it demonstrates the results of our interviews[67] because it can facilitate the recruitment of cybersecurity professionals. It can also make easier communication on cybersecurity among staff members from different departments of a

[61] STEM is Science, technology, engineering, and mathematics.
[62] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map
[63] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf
[64] See for example, https://www.masterstudies.com/Masters-Degree/Cyber-Security/
[65] Ibid.
[66] https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf
[67] Youth IGF TV debate on July 12, available at :
https://www.facebook.com/110382750596633/videos/952725668797866/?__so__=channel_tab&__rv__=all_videos_card

company or administration. By the way, communication on cybersecurity represents a skill in itself and needs to be taught to future professionals.

**➔ University degree offers are quite plentiful in Europe, however a few points need to be underlined regarding the potential difficulties that face employers looking to recruit cybersecurity professionals.**

**First,** the absence of common EU cybersecurity curricular guidelines for higher education lead to a situation in which university offerings are often not in line with current market demand. To take an example, we often see job offer requirements (in addition to IT or technical skills), framed in terms of the knowledge of the project management cycle, establishment of KPI, appropriate communication or ability to communicate large-scale analysis to non-technical audiences. The problem is that IT-focused degrees on cybersecurity (the majority of cybersecurity degrees) do not necessarily offer all these skills to students during their academic studies in cybersecurity. These degrees often have a focus on new defence solutions and the required skills in order to even apply for a cybersecurity job quite often require additional skills that can be accumulated only with practical experience, since these skills do not form part of the academic curricula[68]. This also leads to a situation in which students do not always understand all the professions that exist in cybersecurity, as they focus only on IT or legal cybersecurity degrees. In other terms, there is a need for common EU cybersecurity curricular guidelines that are multi-sectoral, like the cybersecurity field.

> *Cyber security requires a good understanding of law, human factors/psychology, mathematics/cryptography, social sciences, economics, security & risk management/IT audit, etc. Even within the technical domains, there is quite a difference in the skills required for someone working in network/system monitoring, big data/machine learning, digital forensics for a law enforcement agency, malware reverse engineering for a security firm, and performing penetration tests, etc. Ideally, a graduate out of a cyber security programme should have a basic understanding of all those areas, plus an academic background.*[69]

The **first point** leads us to the **second.** The existence of a set of common EU cybersecurity curricular guidelines will also allow more flexibility in terms of the adaptability of the degree offer to market demand, and more flexibility for the admission of students to cybersecurity degree courses. As of today, admission to cyber security degrees (the majority of them are IT-based) requires a number of defined criteria to be met[70]. These criteria are quite often related to technical skills or legal skills (if we refer to cybersecurity degrees in legal studies). This leads to situations, as highlighted by Kathy Liu in an article on the World Economic Forum website, that "by limiting cyber recruitment, hiring and upskilling efforts to IT talent, there are also undesirable spillover effects – such as excluding individuals who tend to be underrepresented in IT to begin with, namely women, minorities and indigenous populations."[71]

[68] We can take as an example this MA curriculum: https://synapses.polytechnique.fr/catalogue/2018-2019/diplome/9/GDCTD-cybersecurity-threats-defenses

[69] https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf

[70] For an example, the following degree: https://www.kcl.ac.uk/onlinecourses/cyber-security?utm_source=google&utm_medium=cpc&utm_campaign=Cyber%20Security&gclid=EAIaIQobChMI28v5lvCz6gIVw-FRCh1NAQLiEAAYAiAAEgK-YfD_BwE&gclsrc=aw.ds

[71] https://www.weforum.org/agenda/2020/05/untapped-cyber-talent-it/

The current figures say that more than 30% of people working in cybersecurity are non-IT specialists[72] or hold no specific cybersecurity degree. This means that 30% of cybersecurity professionals have entered the field vocationally, requiring years to be recognised, or by using non-formal ways of education. This clearly demonstrates that formal education requires more flexibility in cybersecurity education.

The **third point** is chiefly related to the recognition of experience and the role of corporations and industry, which needs to be underlined. Better and closer cooperation with the academic sector will allow better opportunities for students to gain initial experience. The industry has also its role in recognising experience gained and in offering opportunities to gain experience, such as volunteering services to different educational degrees, even those that do not offer a specialisation in cybersecurity (in the absence of cross-sectoral degrees on cybersecurity).

The industry role is also important in supporting media literacy initiatives in cybersecurity that might help to provide students with clearer information on the different professions and cybersecurity employment opportunities that exist in their sectors.

## III. EU CYBERSECURITY EDUCATION GENERAL APPROACH

### 1. Informal track

Here we would like also to gain a consolidated overview of the existing non-formal educational cybersecurity initiatives, such as Red and Blue team events, hackathons and their added value from the perspective of curricula and employment in the sector.

*Lifelong Learning*

Lifelong learning is non-formal learning done at any time of life, which is quite often self-motivated for professional or personal reasons.

“Your generation will need to change and to adapt more quickly, my mum’s generation doesn’t hear about lifelong learning; my generation had to do it, but your generation can’t escape without lifelong learning,” said MEP Marina Kaljurand during her interview with Youth IGF TV[73].

Lifelong learning can take the structured format of specific training or a less structured format, such as an internship or learning by doing. Lifelong learning in cybersecurity represents an interesting way to upskill knowledge on recent cybersecurity trends at any time, but also to obtain certified training, which will allow easier entry to the profession. As Cyber Security

[72] Ibid.
[73] Ibid.

Awards judge Karla Refford has written for Forbes, "…formal education is not the only route into the industry. We know that 81% of hackers are self-taught."[74]

Lifelong learning is also a great opportunity for industry and public authorities to turn black hackers or black hats into white hats and recruit former hackers, through the use of different innovative training formats and upskilling. "Just under half (47%) of under 25s are 'impressed' when they hear about a company being hacked, and a third (33%) are interested in how the hack was conducted." [75] This demonstrates that young professionals are interested in cybersecurity and that their interest needs strongly to be channelled in the right direction: to fighting cybercrime and becoming cybersecurity professionals, rather than criminals. By deploying innovative formats, informal learning has a strong role to play in producing future cybersecurity professionals.

The European Commission has established a Recommendation on Key Competences for Lifelong Learning. This Recommendation was reviewed in 2018[76] and has the objective of supporting and providing an orientation for the development of lifelong learning curricula.
This recommendation lists digital skills as one of the key competences. Digital competence includes cybersecurity awareness. Therefore, it is clear that the European Commission sees digital skills as one of the key competences that EU citizens need to develop during their life.

Influenced by the recommendation or by following the market demand of cybersecurity professionals, market actors have developed a few non-formal ways of education on cybersecurity have been developed by.

*The role of ENISA*

It is important to acknowledge the role of ENISA, the European Union Agency for Cybersecurity, in cybersecurity upskilling activities, and to mention the initiatives established by ENISA, such as the European Cybersecurity Challenge[77]. Launched in 2014, the ECSC is "a cybersecurity competition aimed at increasing talent across Europe and connecting highly skilled individuals with leading industry organisations."[78] The objective of the challenge is to identify and upskill the best cybersecurity IT professionals. It should be noted that only those with a technical background participate in the challenge and the competition is IT cyberskills-focused.

Another initiative is the European Cyber Security Month (ECSM)[79], launched in 2012. Throughout the month of October different actors deploy awareness-raising and educational initiatives or best-practices exchanges on cybersecurity in all EU member states. The Youth IGF has started to help the ECSM expand outside the European Union, specifically by organising cybersecurity activities in the developing world in October.

[74] https://www.forbes.com/sites/forbeshumanresourcescouncil/2019/11/15/is-there-really-a-cybersecurity-skills-gap/#2e02210d10fe
[75] https://media.kaspersky.com/uk/Kaspersky-Cyberskills-Report_UK.pdf
[76] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018SC0014
[77] https://europeancybersecuritychallenge.eu
[78] https://www.enisa.europa.eu/publications/the-status-of-cyber-security-education-in-the-european-union
[79] https://cybersecuritymonth.eu

It will be interesting to go beyond the format of today's ECSM month and turn the activities that are developed by young professionals (often without experience) during the ECSM month into a first experience in cybersecurity that is recognised by industry partners.

This brings us to the question of the recognition of lifelong learning activities and their value in the professional world. In order to be recognised, quite often the activity will need to be certified.

There are a few questions to mention with regard to certification that need to be clarified in the future. What is the certification body and what are the recognised criteria for the certification of a non-formal educational activity? Why and how is the certificate recognised or not by future recruiters (quite often this means industry partners)?

> *So, when we talk about cybersecurity and certifications, I think that the EU can also have a leading role in introducing it within the EU, but also introducing it more widely, more globally. It's better to start with one set of norms and introduce it to the others, then to have a fragmented set of rules in each different country*.[80]

The EU can become a leader not only in online services cybersecurity certification, but also lead this certification in terms of cybersecurity skills or degrees received through the lifelong learning cycle. Cybersecurity skills certification could start with the development of recommendations for a common cybersecurity certification scheme containing at least general criteria. This will reinforce the mobility of the skilled cybersecurity workforce within the EU and allow better cooperation between the private sector and jobseekers.

> *For Europe's digital transformation to be successful it needs to run on trust. As COVID-19 has unfortunately illustrated, significant investment in cybersecurity is required to ensure public support for accelerated digitization. A key element is to ramp up training and certifications for young professionals and students to ensure they are equipped with the essential cybersecurity skills. That is not an easy task and it requires all hands on deck. At Microsoft we are ready to do our part by leveraging our experience and capabilities.*[81]

*CERTs & other initiatives*

There is a need to acknowledge the role of national and regional CERTs[82] in the development of lifelong learning cybersecurity activities.

Depending on the existence of a digital national strategy or a national cybersecurity strategy and national CERT priorities, CERTs can develop a structural training and skills development plan, from activities for youngsters of secondary school age (these can contain competitions, courses and coding activities for girls for example) to higher education (offering courses and

[80] MEP Marina Kaljurand, interview with Youth IGF TV on 2 July, 2020. Ibid.
[81] Casper KLYNGE, Vice-President of Microsoft Corporation, interview with Youth IGF TV, July, 2020.
[82] Computer emergency response team

training sessions, but also certified degrees in cooperation with academic institutions) and professional upskilling (offering certified training)[83].

These focused trainings are often offered in different formats (long or short), based on IT skills or other cybersecurity skills. [84]

It should be noted that the certification of training and degrees is performed by the national CERT itself, as CERTs have developed their own individual schemes and standards for certification of training courses. Training sessions can be free of charge or involve payment.

The different certification schemes used by national CERTs in the EU member states can complicate workforce mobility and recognition of obtained certification by other countries and industry actors, so the role of ENISA and other EU bodies is essential in the development of the guideline for standards for a common EU certification of degrees and cybersecurity skills.

CERTs may choose to initiate Red and Blue team events, a sort of ethical hacking activity developed for the CERT itself or for training or educational activity outside of the CERT.
A team composed of IT professionals or white hat hackers carry out security tests within an organisation by deploying cyber attacks against the organisation's IT network. The Red and Blue teams are quite similar; the Blue teams also analyse the organisation's defence mechanisms. Recognised by the community, the Red and Blue teams concept represents a great option to gain some initial experience in cybersecurity if you are an IT-focused cybersecurity professional. It would be good to have these kinds of initiatives for other cybersecurity skill, as well as for a whole range of hands-on vocational skills, in other words during a real simulation activity.

Among other initiatives, we have to mention the national Cybersecurity Excellent Centres[85], which have the goal of developing national or regional cybersecurity expertise. If developed in all EU member states, these centres can play an important role in the development of cybersecurity skills and informal learning on cybersecurity.

We should also mention the different hackathons, both those developed at EU level, which are open to all member states, and those developed nationally by different public and private actors. The idea of hackathons is to gather different teams of developers interested in cybersecurity solutions for a predetermined period and let them work together to find solutions for an identified cybersecurity challenge.
An activity like this is definitely an upskilling event. However, questions may be raised concerning the recognition of participation in such activity as a professional experience. It would also be interesting to hold cybersecurity hackathons that are not only related to IT solutions, but with a cross-sectoral approach.

➔ **Three points to underline with regard to informal cybersecurity education.**

[83] We can refer here to the UK National Cyber Security Centre, https://www.ncsc.gov.uk/information/certified-training
[84] As in France for example, https://www.ssi.gouv.fr/administration/formations
[85] https://ec.europa.eu/jrc/en/publication/european-cybersecurity-centre-expertise-cybersecurity-competence-survey

Informal cybersecurity education is an interesting and important instrument in creating a cybersecurity workforce. Informal education is more flexible, adaptable and can integrate the rapid changes in demand on the workforce market, as well as the fast-moving challenges facing the cybersecurity sector. "We have jobs that we could not even think of a couple of years ago," MEP Eva Kaili told Youth IGF TV. "I remember a friend of mine who told me: 'Listen, my daughter told me she wants to be a YouTuber, and I was really shocked.' And of course, there is no class; there are no lessons that prepare you for that. You have to add more qualifications in order to be able to be successful."[86]

Today, the majority of formal and informal cybersecurity education is focused on IT or legal skills. The market is clearly in demand of cross-sectoral cybersecurity skills; tomorrow we can imagine the demand for a cybersecurity communicator for example. Informal education will be an essential element in providing new skills where formal cybersecurity education is not yet present. Innovative lifelong learning formats can also help with two problematic elements of the cybersecurity workforce market: the difficulties faced in gaining entry to the profession by entry-level professionals without experience[87] and the problem of retaining cybersecurity professionals in their positions.

However, three points seem to be important related to informal cybersecurity education.
**Firstly**, it is important that industry players recognise informal educational initiatives as being professional experience. By participating in designing these initiatives and developing closer cooperation with the actors in charge of the initiatives, industry representatives can be sure of the quality standards of the information delivered and upskilling schemes, since they can participate in their design. This will facilitate the recruitment of entry-level professionals and make it easier to retain existing cybersecurity staff, as well as allowing those interested in entering the cybersecurity field the flexibility of changing their career. This approach can also allow job offer requirements to be adapted in line with existing cybersecurity skills.
If the industry wants to participate in reducing the cybersecurity gap, it clearly needs to have company cross-department cooperation on cybersecurity skills programmes and to open up for cooperation, with different external actors delivering informal cybersecurity education.

**Secondly**, to facilitate the recognition of informal cybersecurity education as professional experience, as well as upskilling by different partners, the industry sector needs to be helped by other bodies. In the EU, developing recommendations for common guidelines on criteria and standards for certification of cybersecurity lifelong learning initiatives and degrees can be done by EU bodies in collaboration with the multi-stakeholder community.

**Thirdly**, it might be helpful to develop a common EU database for lifelong learning cybersecurity initiatives, similar to the one developed by ENISA for higher education degrees[88]. This will facilitate an understanding of the informal cybersecurity activities that exist in the EU member states for people looking for this kind of activity. It will also provide clarification for industry partners that might make it easier for these informal activities to be recognised as professional experience during the recruitment process.

[86] MEP Eva Kaili, interview with Youth IGF TV on 7 July, 2020, Ibid.
[87] https://www.forbes.com/sites/forbeshumanresourcescouncil/2019/11/15/is-there-really-a-cybersecurity-skills-gap/#66933ecf10fe
[88] Cybersecurity Higher Education Database.

# CONCLUSION

"Cyber has become many-faced and has many different layers. I'm a lawyer by education, I'm a diplomat, I'm a former Foreign Minister, but I'm dealing with cybersecurity. I'm not an IT expert, but I can bring to cybersecurity relations between states. (…)…. We all need to be IT experts,"[89] said MEP Marina Kaljurand during her interview with Youth IGF TV on 2 July, 2020.

Our brief assessment demonstrates that a fragmentation of cybersecurity skills curricula is taking place. What we can see today is that the existing educational tracks on cybersecurity offer sectoral education, i.e. they are oriented towards sector-oriented professions: IT professionals, legal professionals and, to a very limited degree, policy/diplomacy. However, the rapid development of the digital space and the role that digital technology is taking in our lives, especially as demonstrated by the coronavirus crisis, requires cybersecurity skills to be cross-sectoral and not only focused on one specific skill. In order to be able to produce adequate cybersecurity professionals that will answer the workforce market demand and to eliminate the cybersecurity gap, the EU urgently needs to take a lead on cybersecurity skills and re-think formal and informal cybersecurity education.

Private sector and corporations can help in harmonising cross-sectoral cybersecurity education to facilitate a structured EU-based approach towards the cybersecurity skills agenda. By investing in a cybersecurity skills-structured approach and initiatives, the private sector can facilitate the development of policies on cybersecurity skills within the EU. Today's post-corona moment can be fruitful for such a collaboration, as "the New Action Plan[90] will enhance and support digital skills for Europe. … The new strategic planning for Europe for the next seven to ten years, I would say, will happen under the prism of green technology, digitalisation and this includes artificial intelligence of course and digital skills."[91]

The European Skills Agenda[92], which is under review now, entered into the ongoing open consultation process, needs to develop a structured EU approach on cybersecurity skills. The role of all stakeholders is crucial to achieving this goal.

> *It [the EU Skills Agenda] touches twelve actions that are organised around very interesting topics. So one is (…) to make sure that people will have the right skills for jobs, to ensure that they can make the transition to another job and that they acquire skills fully, free and very, very fast. (…)*
> *(…) so to equip all of us with these digital skills is needed now more than ever. So now is the best time to have an ambitious digital skills agenda. We estimate that 70% of jobs will need digital skills and you need to be able to acquire them easily, at least in the European Union[93]*.

[89] Ibid.
[90] Should be read as the New Education Digital Action Plan, https://ec.europa.eu/education/education-in-the-eu/digital-education-action-plan_en
[91] MEP Eva Kaili, interview with Youth IGF TV on 7 July, 2020, Ibid.
[92] https://ec.europa.eu/social/main.jsp?catId=1223&langId=en
[93] MEP Eva Kaili, interview with Youth IGF TV on 7 July, 2020, Ibid.

## RECOMMENDATIONS FOR ACTION

**Here we would like to present the recommendations made by young people from the Youth IGF for an efficient EU cybersecurity skills agenda.**

| POLICY ACTION | DEVELOPMENT ACTION |
| --- | --- |
| 1. Promote and encourage media literacy on cybersecurity at the EU level | 1. Promote upskilling initiatives recognised by the industry that will focus on cross-sectoral cyber skills. |
| 2. Establish and promote a common EU cybersecurity skills curricular guidance or a recommendation for guidance on cybersecurity skills curricula for different formal education levels that can be recommended to the member states. | 2. Facilitate the development of a set of guidelines for employers on on ensuring descriptions of cybersecurity job offers are up-to-date and written in language comprehensible for entry-level professionals, HR departments and cybersecurity departments. |
| 3. Support existing volunteering actions for the young at the end of their studies and encourage the development of new ones within EU institutions working on cybersecurity, like Cybersecurity EU volunteers. This can also be done as an upskilling mechanism, to help the young gain their first experience in the field and to promote learning by doing. | 3. Facilitate and encourage the development of learning concepts for teaching cybersecurity skills to pupils (of different age groups). |
| 4. Call for a common EU certification for cybersecurity skills training modules (e.g. under one of the priorities of the digital skills agenda, in collaboration with ENISA). | 4. Facilitate the development of the recommendation for better internal communication (or intra-departments) on cybersecurity skills for industry. |
| 5. Improve the dialogue in between EU institutions and the young on cybersecurity by initiating an annual (physical/or virtual) meeting and through initiatives such as the Youth IGF. | 5. Better public-private-youth dialogues on cybersecurity topics in the EU context. |