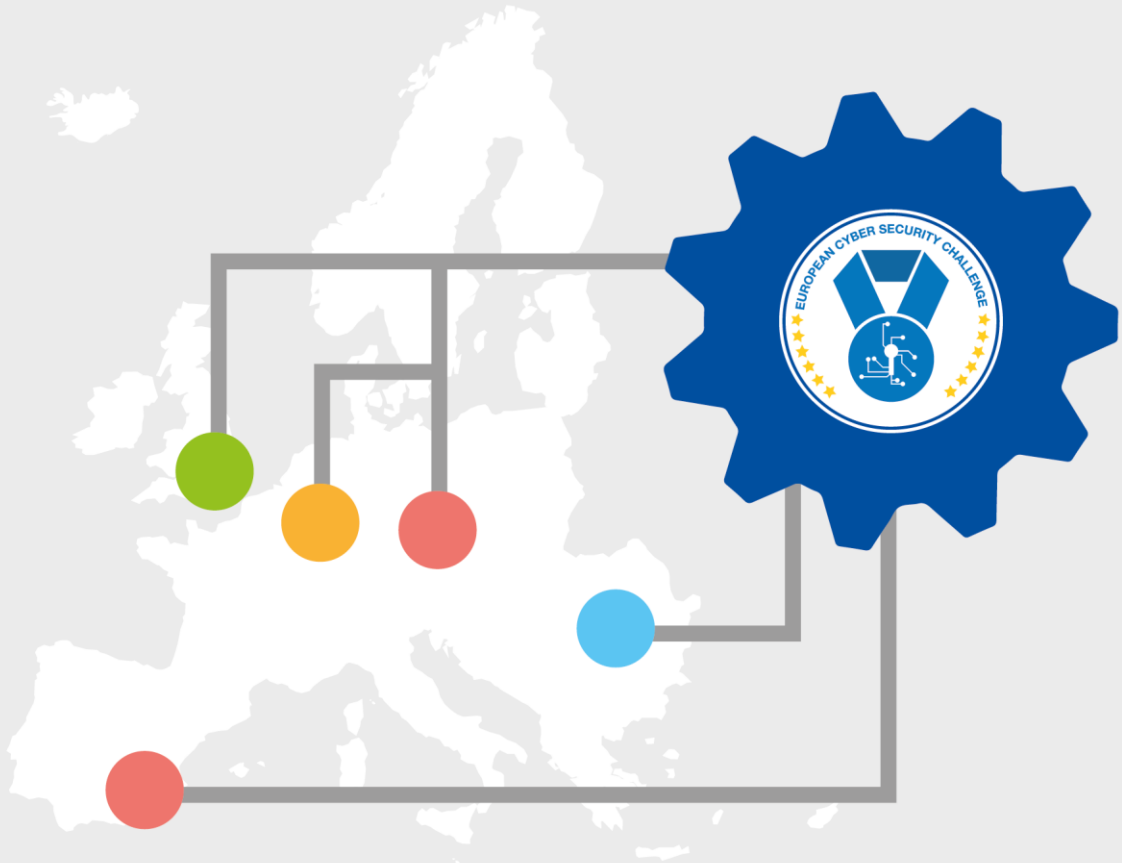
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



TOWARDS A COMMON ECSC ROADMAP

Success factors for the implementation of national cyber security competitions

APRIL 2021

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

EDITORS

Adrian Belmonte, Fabio Di Franco – European Union Agency for Cybersecurity

AUTHORS

Tommaso De Zan — tommaso.dezan@linacre.ox.ac.uk
Muhammad Mudassar Yamin— muhammad.m.yamin@ntnu.no

Both authors are listed alphabetically and they contributed equally to the report

ACKNOWLEDGEMENTS

The authors would like to thank the ECSC Sterring Committee for their participation in this research and their insightful comments.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-464-0 – DOI: 10.2824/657311

EXECUTIVE SUMMARY

This report aimed to identify the key factors enabling the success of a national cyber security competition and to give a snapshot of the current situation in the EU and ECSC partner countries. To do that, we conducted a dozen of interviews with national and EU experts, searched and reviewed the relevant scientific literature and collected data on these key enabling factors with a survey, which was filled by 90% of the countries attending the ECSC. This was done to provide preliminary insights and a discussion platform to determine a common ECSC roadmap.

In light of this research, we believe that establishing and implementing a common ECSC roadmap with a view to promote a standardisation of national cyber security competitions has the potential to make the ECSC the EU flagship policy in the field of cyber security education. This would place the ECSC in a primary position to support the objectives of the EU Security Union Strategy for the period 2020-2025. We believe so because we currently do not see many other policies that, like the ECSC, could potentially involve 20.000 students, provide solid cyber security training to almost 1.000 individuals and give such visibility to EU efforts in cyber security policies.

The interviews with national experts and the survey found that the main objectives a national competition should meet are:

- Identify young cyber security talent
- Increase interest in cyber security as a topic
- Increase cyber security knowledge and skills
- Increase interest in a cyber security career and connect participants with employers
- Create a network of young cyber security specialist

National experts identified six main factors that are conducive to achieve these objectives (section 3), namely:

- Policy relevance
- Governance and Public-Private Partnership (PPP)
- Funding
- Public relations and marketing strategy
- Organization, training and cyber security challenges
- Connection with employers and career outcomes

Based on the survey results on these key enabling factors (section 4) and an analysis of these results (section 5), this report provides recommendations for the establishment of a common ECSC Roadmap (section 6), if stakeholders wish to develop the ECSC to its fullest potential.

TABLE OF CONTENTS

1. INTRODUCTION 5

1.1 SCOPE OF THE REPORT 5

1.2 TARGET AUDIENCE 6

1.3 STRUCTURE OF REPORT 6

2. BACKGROUND AND CONTEXT 7

2.1 POLICY FRAMEWORK OF CYBER SECURITY EDUCATION IN THE EU 7

2.2 THE GENERAL CONTEXT OF CYBER SECURITY COMPETITIONS 8

2.3 SHORT HISTORY OF ECSC 10

3. IDENTIFICATION OF KEY ENABLING FACTORS 12

3.1 INTERVIEWS WITH NATIONAL EXPERTS AND LITERATURE REVIEW 12

3.2 RESULTS OF INTERVIEWS AND LITERATURE REVIEW 12

3.2.1 Policy relevance 14
3.2.2 Governance and PPP 14
3.2.3 Funding 16
3.2.4 Public relations and marketing strategy 16
3.2.5 Organization, training and cyber security challenges 17
3.2.6 Connection with employers and career outcomes 21

4. CURRENT STATUS OF NATIONAL CYBER SECURITY COMPETITIONS 22

4.1 NATIONAL CYBER SECURITY COMPETITION OBJECTIVES 22

4.2 POLICY RELEVANCE, GOVERNANCE AND PPP 22

4.3 FUNDING 24

4.4 PUBLIC RELATIONS AND MARKETING STRATEGY 25

4.5 ORGANIZATION, TRAINING AND CYBER SECURITY CHALLENGES 25

4.5.1 Recruitment and phases of the competition 25
4.5.2 Cyber security challenges, training and technological infrastructure 30

4.6 CONNECTION WITH EMPLOYERS AND CAREER OUTCOMES 33

5. OPPORTUNITIES AND CHALLENGES FOR A COMMON ECSC ROADMAP 35

5.1 NATIONAL CYBER SECURITY COMPETITION OBJECTIVES 35

5.2 POLICY RELEVANCE, GOVERNANCE AND PPP 36

5.3 FUNDING 37

5.4 PUBLIC RELATIONS AND MARKETING STRATEGY 38

5.5 ORGANIZATION, TRAINING AND CYBER SECURITY CHALLENGES 38

5.5.1 Recruitment and phases of the competition 38
5.5.2 Cyber security challenges, training and technological infrastructure 40

5.6 CONNECTION WITH EMPLOYERS AND CAREER OUTCOMES 41

5.7 ENISA'S ROLE 42

6. CONCLUSIONS AND RECOMMENDATIONS 43

6.1 POLICY RELEVANCE, GOVERNANCE AND PPP 45

6.2 FUNDING 45

6.3 PUBLIC RELATIONS AND MARKETING STRATEGY 46

6.4 TRAINING AND THE COMPETITION 47

6.5 CONNECTION WITH EMPLOYERS AND CAREER OUTCOMES 48

6.6 ENISA'S ROLE 48

1. INTRODUCTION

There is a shortage of cyber security professionals in the labour market. According to the latest figures, the 2020 cyber security workforce gap lies at 3.1 million worldwide, with 56% of security experts thinking that cybersecurity staff shortages are putting their organizations at risk. Other estimates suggest that the global cyber security workforce would need to grow by 89% if organizations were to defend their critical ICT assets effectively.[1]

Against this background, governments have implemented various programs and policies to increase the number of professionals entering the cyber security labour market. National cyber security competitions (NCSCs), in the form of capture the flag events among teams of students, have been among the most widespread tools to address the cyber security skills shortage. There are now several national cyber security competitions worldwide, including in Asian, English-speaking and European countries. The European Union (EU) organizes through the European Union Network and Information Security Agency (ENISA) and the European Commission (EC), the European Cyber Security Challenge (ECSC). The ECSC is the pan-European cyber security competition that aims at enhancing cybersecurity talent across Europe and connecting high potentials with industry leading organizations.[2] The latest edition of the ECSC, in 2019, took place in Romania and saw the participation of approximately 200 young cyber security specialists and 20 national teams.[33]

In this context, ECSC stakeholders have started to reflect upon ways to strengthen and improve ECSC outcomes. At end of each year's competition, ENISA produces an "ECSC Analysis Report" where it analyses lessons learnt about the current ECSC in relation to past editions. However, these reports focus only on the planning and implementation of the ECSC and not on the various national cyber security competitions that select the participants who will later attend the ECSC.

Against this backdrop, ECSC stakeholders aim to deepen their understanding of the key elements that make a national cyber security competition successful and therefore strengthen the outcomes of both national competitions and the ECSC.

1.1 SCOPE OF THE REPORT

The objectives of this report are to identify the key success factors of a national cyber security competition, collect data on these key factors and provide an overview of the current status of national cyber security competitions in the EU and ECSC partner countries.

The expected impact of this report is to provide national organizers with preliminary insights and an evidence-based platform to discuss the realization of a common ECSC Roadmap. In doing so, the report will highlight the technical and organizational factors that are necessary for the implementation of a Common ECSC Roadmap and will provide policy recommendations for both the short term and long-term implementation of this Common ECSC Roadmap.

[1] https://www.isc2.org/-/media/ISC2/Research/2020/WorkforceStudy/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07
[2] https://europeancybersecuritychallenge.eu/about
[3] https://europeancybersecuritychallenge.eu/archive

1.2 TARGET AUDIENCE

The target audiences of this report are:

- The organizers of the national cyber security competitions that select team attending the ECSC;
- The EU institutions involved in the organization and planning of the ECSC, most notably ENISA and the EC;
- The stakeholders that benefit from the success of national cyber security competitions, including academia, national governments and the private sector.

1.3 STRUCTURE OF REPORT

This report is organized as follows:

- Section 1, “Introduction,” gives an overview of the report, states its objectives and target audiences;
- Section 2, “Background and context,” puts national cyber security competitions and the ECSC in perspective;
- Section 3, “Identification of key enabling factors,” presents the most important elements that national and EU experts have identified as conducive to the success of national cyber security competitions;
- Section 4, “Survey results,” collects data on these key factors from national cyber security competitions leading to the ECSC; in doing so, it provides an overview of the current status of national cyber security competitions based on the key factors identified by experts;
- Section 5, “Opportunities and challenges for a Common ECSC Roadmap,” analyses the survey results in light of section 3;
- Section 6, “Conclusions and recommendations,” summarizes the report and provides short- and long-term recommendations for the realization of a Common ECSC Roadmap based on the analysis of section 5.

2. BACKGROUND AND CONTEXT

2.1 POLICY FRAMEWORK OF CYBER SECURITY EDUCATION IN THE EU

The EU started to devote interest in cyber security education and skills since the publication of the of the first EU cybersecurity strategy in 2013, when member states were encouraged to increase efforts in education and awareness activities in network and information security topics.[4]

In the 2017 Joint Communication "Resilience, deterrence and defence: Building strong cybersecurity for the EU," the EU reiterated that "there is a strong education dimension to cybersecurity" and that "effective cybersecurity relies heavily on the skills of the people concerned." In the Communication, the EU pledged to develop cyber security skills by building on the work of the Digital Skills and Job Coalition and by establishing a European cybersecurity industrial, technology and research competence centre, as well as a network of national cybersecurity coordination centres.[5]

The EU has been an active player in the development of cyber security skills and the new EU Security Union Strategy puts skills and awareness raising under the spotlight.

In 2019, four consortiums – CONCORDIA, ECHO, SPARTA and CyberSec4Europe – received financial support from the EU to run pilot projects for the establishment of a European cybersecurity competence network and the development of a common European cybersecurity research and innovation roadmap. Since their inception, these consortiums have been conducting various activities in the field of cyber security education and skills. For example, they have produced reports on cyber security workforce diversity and a feasibility study on cyber security skills certifications;[6] they plan to publish a cyber skills framework and an overall cyber security education and training framework.[7]

In 2020, the EU Security Union Strategy dedicated an entire section on skills and awareness raising, which posits that awareness of security issues and the appropriate skills are necessary to build a more resilient society. In the context of the growing reliance on ICT following the Covid-19 Pandemic, threats to IT systems and networks show the need to improve human capacity to deal with such issues. The Strategy indicates that programs such as the Digital Education Action Plan, Digital Europe Program and the future European Research Area and European Education Area will need to include specific measures to build IT security skills in the population.[8]

Against this background, ENISA has an important role in the development of cyber security education and skills in the EU. Besides applied research and studies in topics such as NIS education, public–private partnerships in education and workforce development, the EU cybersecurity agency has a leading role in the organisation and implementation of the European Cyber Security Month, an EU-wide awareness campaign fostering cybersecurity knowledge

[4] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/cybercrime/docs/join_2013_1_en.pdf
[5] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en
[6] https://www.concordia-h2020.eu/deliverables/
[7] https://echonetwork.eu/echo-cyberskills-framework/
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0605&from=EN

among citizens through the promotion of education, sharing of good practices in data and information security.[9]

Most recently, ENISA has also launched the Cybersecurity Higher Education Database, an interactive map that lists and provides useful information on cyber security degrees across Europe. The Database aims to become the main point of reference for all citizens looking to upskill their knowledge in cybersecurity in the EU[10]. Furthermore, the Agency is in the process of developing a European Cybersecurity Skills Framework, whose objective is to create a common understanding of roles, competencies, skills and knowledge in the field of cyber security with a view to address the lack of cyber security professionals in the labour market.[11]

Finally, and most importantly for the purpose of this report, ENISA organizes together with the European Commission and member states the European Cyber Security Challenge, the EU cybersecurity competition aimed at increasing talent across Europe and connecting highly skilled individuals with leading industry organisations.[12]

2.2 THE GENERAL CONTEXT OF CYBER SECURITY COMPETITIONS

National cyber security competitions have been increasingly used as a tool by governments around the world. There are several objectives that national cyber security competitions are touted to achieve, including encouraging young people to pursue a cyber security career, nurturing students' interest, attracting talented individuals to the field and, ultimately, meeting cyber security skills demands to generate a self-sustained cyber security workforce.

Table 1: Cyber Security Competitions Key Objectives according Countries in the Five Eyes Intelligence Alliance

Country and Author	Quote
Australia	*"Expanding the national annual Cyber Security Challenge Australia (…) will also help generate a sustained national pipeline of cyber security professionals."*[13]
Canada	*"Youth are a vital talent pool to meet cyber security skill demands" and "This collaboration of National Youth Cyber Education Programs seeks to promote education and awareness in technology education and foster excellence in students pursuing careers in cyber security or other science, technology, engineering, and mathematics (STEM) areas."*[14]
European Union	*"The European Cyber Security Challenge is an initiative by the European Union Agency for Cybersecurity (ENISA) and aims at enhancing cybersecurity talent across Europe and connecting high potentials with industry leading organizations."*[15]
United Kingdom	*The Initial Strategy cites Cyber Discovery as a program aimed at supporting skills capability "by identifying and engaging young people and nurturing their interest in cyber security as a future career path."*[16]
United States	*"Cybersecurity competitions have been increasingly popular tools for attracting talented individuals and federal agencies should make greater use of them, including for professional development."*[17]

[9] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cyber-security-month
[10] https://www.enisa.europa.eu/topics/cybersecurity-education/education-map
[11] https://www.enisa.europa.eu/topics/cybersecurity-education/european-cybersecurity-skills-framework
[12] https://www.enisa.europa.eu/topics/cybersecurity-education/eu-cyber-challenge
[13] https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf
[14] https://www.cybertitan.ca/index.php/about/what-is-cybertitan/
[15] https://europeancybersecuritychallenge.eu/about
[16] https://tinyurl.com/y5thpmwm
[17] https://www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf

There are various examples of national cyber security competitions that are now an integral component of governments' cyber security workforce development strategies, most notably in English-speaking and European countries.

Cybersecurity competiotions have been implemented worldwide with the goal to reduce the shortage of cyber security professionals

For example, Australia extensively deploys cyber security competitions such as CyberTaipan, which is a competition open to young people between 12-18 years-old with an interest in cyber, defence, puzzles and code breaking. It is organized in several rounds and the winning teams represent their schools at the national finals. The objectives of the organizers are: 1) to improve both awareness of and interest in cyber security careers and education pathways; 2) improve fundamental technical cyber security skills.[18] According to a senior industry leader involved in the organization of such competitions: "STEM education is vital to the future of Australia and its national security. Programs such as CyberTaipan play an important role in teaching not only technical skills, but also professional skills such as leadership, communications, collaboration and teamwork."[19]

In the UK, Cyber Discovery is a government-funded extracurricular programme for secondary students aged 13-18 to ensure that as many people as possible enter the cyber security profession in the coming years.[20] Cyber Discovery is a free-online programme which is designed around four phases. Students who score the highest in the four phases are then invited to a final on-site bootcamp/capture-the-flag event. In the first edition of the programme in 2018, nearly 24,000 students signed up to the first phase, while 170 were then invited in a face-to-face training bootcamp in Manchester.[21] The program is among the policy interventions foreseen in the "Initial Cyber Security Skills Strategy" and has a budget of £20 million. According to the UK government: "Cyber security is an integral part to the UK making the most of the digital age, and programmes like Cyber Discovery and the NCSC's CyberFirst are helping young people develop skills that lead to dynamic and rewarding careers. Investing in these initiatives will make a huge difference for generations to come, and will help us to find and support motivated, high performers from all backgrounds who want to make a positive impact on the world."[22]

In the US, three national cybersecurity competitions: CyberPatriot, the Collegiate Cyber Defense Competition (CCDC), and U.S. Cyber Challenge (USCC), have been targeting different communities, from middle schoolers to professionals already in the workforce. The CyberPatriot program was introduced in 2009 to draw more young women and men to education and careers in cybersecurity and STEM fields with a view to meet the needs for an increasingly technical workforce. In the 2018-19 edition, 24,139 students participated in the cyber defense competition, significantly up from the 2010-11 edition when 3,635 students attended. [23]

In the EU, the EC and ENISA coordinate and support the ECSC, which aims at "enhancing cyber security talent across Europe and connecting high potentials with industry leading organizations." It is based on the premise that "growing need for IT security professionals is widely acknowledged worldwide" and many countries in the EU have organized cyber security competitions "with a clear aim to find new and young cyber talents and encourage young people to pursue a career in cyber security" and "to help mitigate this shortage of skills." The ECSC also has broader goals: it places cyber security at the service of humankind by promoting a peaceful society, it fosters friendly relations among attending countries, it promotes diversity in

[18] https://www.austcyber.com/educate/competitions-and-challenges
[19] https://news.northropgrumman.com/news/releases/northrop-grumman-celebrates-successful-pilot-of-australian-cybertaipan-competition
[20] https://medium.com/cyber-discovery/about
[21] https://medium.com/cyber-discovery/cyber-discovery-launches-the-first-cyberstart-elite-camp-in-manchester-f9860b59e7d and https://medium.com/cyber-discovery/year-2-whats-new-4442efd4df8a
[22] https://tinyurl.com/y5thpmwm
[23] https://www.afa.org/content/dam/afa/national-convention/CyberPatriot%20Impact%20Report_2019.pdf

cyber security and overall it sustains EU policies to combat cybercrime and on cyber security more generally.[24]

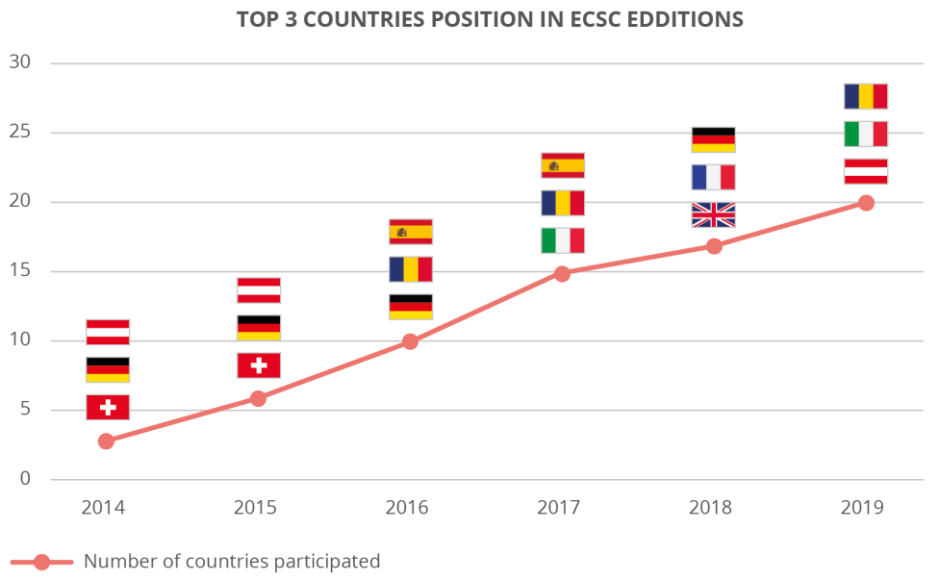
2.3 SHORT HISTORY OF ECSC

The ECSC is the annual pan-European and multinational cyber security competition where national teams of young individuals aged between 16-25 years-old compete against each other in a capture the flag (CTF) event, which typically involves challenges in domains such as web security, mobile security, crypto puzzles, reverse engineering, and forensics.

The first edition of the ECSC took place in Austria in 2014, when three national teams – Austria, Germany and Switzerland – competed against each other in challenges such as APT network forensic, java hash collisions, HQL injections and license key circumventions. In the same year, ENISA conducted a study to identify the status of cyber security competitions which were active at that time.[25][25] The report described the experiences of 5 different national cyber security competitions (Austria, Romania, Spain Switzerland and United Kingdom) and outlined a roadmap for a pan-European cybersecurity competition. The study recommended to establish a European Cyber Security Challenge similar to the UEFA football league, whereby each member state organizes a local national competition and the winners of these competitions are then selected to attend the ECSC. The report provided guidelines and recommendations for the implementation of such competitions with a focus on the establishment of a public private partnership to increases cyber security awareness among Europeans and help identifying young cyber security talent.

Since then, the ECSC has expanded each year. In the second edition of ECSC (2015), 6 countries attended, namely Austria, Germany, Spain, Romania, UK and Switzerland. The number of participants rose to 10 in the 2016 edition. In the latest 2019 edition a total of 20 European countries gathered in Bucharest, Romania. The expansion of the ECSC with respect to the number of countries which participated and the top 3 position holders in those competitions is presented in Figure 1.

Figure 1: Number of countries attending the ECSC and top 3 position holders over the years



[24] https://europeancybersecuritychallenge.eu/about
[25] Cyber security competitions — the status in Europe (2014, October). Retrieved November 15, 2020, from https://www.enisa.europa.eu/publications/cybersecurity-competitions-2014-the-status-in-europe

To participate in ECSC each country organizes a local national competition in order to select a national team,. Multiple factors are involved in the success of national competitions. One of the objectives of this report is to identify the key factors enabling the success of national cyber security competitions, which is the focus of the following chapter.

3. IDENTIFICATION OF KEY ENABLING FACTORS

3.1 INTERVIEWS WITH NATIONAL EXPERTS AND LITERATURE REVIEW

This research seeks to identify the key factors enabling the success of national cyber security competitions through two different methodologies, namely interviews with the national organizers of those cyber security competitions leading to the ECSC and a review of the relevant literature.

The researchers conducted 14 in-depth, semi-structured interviews with organizers of national cyber security competitions between June and July 2020. Questionnaires were sent to the national representatives who sit in the ECSC Steering Committee: 12 national organizations replied to the request for interview. The 12 national organizations which were interviewed represent 60% of countries sitting in the ECSC committee and approximately 282 million of the European population. In addition, 2 representatives from EU institutions involved in the ECSC were also interviewed.

Interviews were divided in two parts. In the first part, interviewees were asked to list the objectives of their national competitions, pair them with the indicators that their organizations use (or would use) to measure success and finally the most important factors to achieve these objectives. In the second part, interviewees were asked to list the 5 most important objectives a generic national cyber security competition should have (thus regardless of the objectives of their specific national cyber security competitions) and questions on important factors that had been identified in the literature.

This report identifies the key factors enabling the success of national cyber security competitions through in-depth interviews with national and EU

The researchers also identified key enabling factors for the success of competitions through a literature review. The relevant literature was found using a keyword-based technique: the keywords “cybersecurity competitions” were searched in the “Google Scholar Database”, which provides the meta indexing of the most relevant academic databases such as IEEE, ACM and Springers. At the moment of the search (July 2020), the researchers found 265 entries related to the keyword “cyber security competitions.” Following a review, 25 publications were selected based on their relevance and were analysed in-depth.

3.2 RESULTS OF INTERVIEWS AND LITERATURE REVIEW

Interviews found that national cyber security competitions generally attempt to achieve 4 main objectives:

- Increase participants’ cyber security skills and knowledge;
- Identify young cyber security talent, including forming the national team attending the ECSC;
- Develop interest in cyber security as a topic and career possibility;
- Promote cyber security awareness among participants and the wider population.

Organizers also mentioned other objectives that their national cyber security competition try to achieve, but there was usually less consensus compared to the four objectives listed above. These other complementary objectives are:

- Increase the number of individuals attending the national competition;
- Create a community of young cyber security experts;

- Promote diversity;
- Promote moral values such as transparency and other ethical principles;
- Encourage open knowledge.

Finally, national experts also mentioned other higher-level aims such as influencing the modernization of the national education system and protecting a country's IT infrastructure. National organizers identified several indicators to measure whether the competition achieves "success" according to these objectives. This report concentrates solely on the first 4 objectives:

- Indicators of success for **"Increase participants' cyber security skills and knowledge"**:
  - Participants can compete and complete most challenges provided
  - Number of challenges that are solved by participants
  - Participants better understand cyber threats and risks
  - Higher ranking in international challenges and competition (including the ECSC)
  - Amount of new learning content produced each year
  - Participants' performance in future CTFs
  - Number of participants with above average results in each competition's round
  - Results of feedback questionnaire sent to participants
- Indicators of success for **"Identify young cyber security talent, including forming the national team attending the ECSC"**:
  - Number of participants attending the national cyber security competition
  - Number of new participants attending the national cyber security competition
  - Number of participants and actively involved in solving challenges
  - Ranking in international challenges and competition, including the ECSC
- Indicators of success for **"Develop interest in cyber security as a topic and cyber security careers":**
  - Participants establishing new local CTF teams
  - Participants founding new companies
  - Participants are actively involved on the competition's platform
  - Career fairs are organized and are well attended
  - Participants obtaining internships or receiving job offers after the competition
  - Participants enrolling in a cyber security degree
  - Increased demand for cyber security educational programs
  - Number of interviews for cyber security jobs that participants undergo
- Indicators of success for **"Promote cyber security awareness among participants and the wider population"**:
  - Number of participants in the first round of the competition
  - Number of cyber security discussions in schools
  - Diffusion of communication strategy and social media presence
  - Awareness conferences are organized and well attended

The report identified six main factors that are conducive to the success of a NCSC

National organizers identified **six main factors** that are conducive to achieve the objectives listed above, which are:

1. Policy relevance
2. Governance and Public-Private Partnership (PPP)
3. Funding
4. Public relations and marketing strategy
5. Organization, training and cyber security challenges
6. Connection with employers and career outcomes

Below, we explain why each of these factors is relevant for the success of a competition based on the explanations provided by national experts during interviews. These factors are not listed or described in order of importance and are presented independently from any of the objectives

above. This is done because many of these factors could help reach more than one objective at the same time and therefore should be not seen in isolation from each other.

3.2.1 Policy relevance

Although not everyone considers it necessary or even desirable, organizers generally suggest that it is a good sign for a national cyber security competition to have a certain "policy relevance" and for it to be aligned with or mentioned in the country cyber security strategy. This because a national cyber security competition is viewed as a potential solution to mitigate a country-level issue such as the cyber security skills shortage. According to one national expert: "A competition is a relatively easy and practical way to address the cyber security skills shortage, in a qualitative as well as quantitative sense. It would be one of the interventions under the more general topic of capacity building." Another interviewee adds that "cyber security education should be in the strategy of every country. Enhancing the average knowledge in cyber security and addressing the skills-gap in this area is paramount for the security of a country."

Experts believe that a NCSC should be aligned with a country national cyber security strategy

A competition that is policy relevant has the benefit to: "gain credibility and prestige; obtain a bigger impact and scope; be more stable and adopt a medium-long term strategy; obtain financial resources more easily." According to one organizer, a national competition should be coordinated with the government's strategy on the basis of market demands and the country needs, so that "the competition can be improved and adapted every year, in a changing and rapidly evolving environment." A national cyber security competition that selects the team attending the ECSC should be a strategic national policy and goal and should clearly distinguish itself from any other CTFs. As one interviewee notices, countries should "make the competition stand out by being THE official qualifier for the ECSC."

As an example of "policy relevance", one organizer pointed out that the Italian Minister of Defence and the National Intelligence Chief usually participate in the award ceremony of his national competition and later the national team attending the ECSC is received by the Prime Minister. Policy relevance is also achieved when the various national ministries, and not only the main national cyber security agency, are on board and collaborate to support the competition. One interviewee feels that overall the "support of national institutions is essential."

3.2.2 Governance and PPP

It was clear from interviews that a perfect governance setting does not exist and that the governance formula of any national cyber security competition depends on several national factors such as for example the presence or not of a dedicated national cyber security agency, funding arrangements, maturity of the national cyber security industry and overall cyber security posture of a country. As one interviewee put it "there is no ideal approach in our view. They all have positive and negative aspects."

Nonetheless, it is important for a national cyber security competition to have a clear governance structure in place as this heavily shapes the competition's objectives and outcomes. Even though there was consensus on the absence of a fixed governance formula, there was a certain convergence on the idea that a Public-Private Partnership (PPP) involving the key actors of the national cyber security ecosystem provides numerous benefits to a national cyber security competition. One interviewee stated that the majority of "success stories come from partnerships between government, academia and NGOs," while another interviewee reflected that "it does not matter who is the leader, it is important to work together."

The scientific literature has also highlighted various benefits of a public-private partnerships. According to researchers, a PPP can play a vital role in managing and updating the competition according to workforce requirements and provide a win-win collaboration scheme for both the public and the private sector. For example, researchers found that [26][27] technical capabilities and expertise from different academic and non-academic institutions could further assists the development of challenges in future cyber security competitions. This may include incorporating real life cyber security incidents happening in government and private sector, thus making cyber security competitions more relevant to different stake holders.

Organizers also perceive that it is important for governments to be in the front line and support national competitions, especially when these are in their "start-up phase." Initial government support is needed to avoid the overall message being "hijacked" in favour of other competing objectives that other actors might have. In sum, "the best way would be a balanced or mixed model where the government leads the national competition in cooperation with the cyber ecosystem." Ideally, some sorts of grassroots community/NGO/foundation or academia should be responsible for the organization and implementation of the challenge, provided they have the necessary know-how. The benefit of having such actors sitting in the front seat would be their independence. Moreover, interviews underlined that it is of essence to involve the private sector and cyber security practitioners in the competition through various activities, although there is no consensus on the type of involvement industry should have. For some, companies should provide trainings to participants, for others they should provide the online infrastructure or directly fund the competition.

Governments should be supporting NCSCs, especially when they are in their "start-up" phase

Against this background, national organizers think that national cyber security competitions should be well connected to the rest of the national cyber security ecosystem. In this sense, it is not only a question of governance and who "controls" or implements a cyber security competition. Rather, it is a question of whether and to what extent a national competition is systematically connected to other relevant cyber security actors and the kind of synergies that these connections create. Because competitions bring together security researchers, professionals, academia, students and companies they contribute "to the reduction of the complexities of the public–private cooperation and increase the visibility of cybersecurity in public strategies on a national level." Moreover, having links with the rest of the ecosystem is important to build a network of "friends" willing to contribute to the development of young cyber security experts and to look for synergies in the identification of the best talent in the country.

Connecting the various dots of the ecosystem can be advantageous for participants, who will potentially fill roles required by any national cyber security strategy in the future. For the competition, it is an advantage to be part of the ecosystem too as this can be helpful to find other sources of funding and to connect participants with companies. Endorsement of key ecosystem players can help to attract newcomers and make the competition more exciting for senior participants. But this relationship can be valuable to the industry as well, as "involving more actors is the right way, not only in cost saving terms but also because of the importance that this relationship with the ecosystem brings up to promote and foster the cybersecurity industry."

[26] Burns, T. J., Rios, S. C., Jordan, T. K., Gu, Q., & Underwood, T. (2017). Analysis and Exercises for Engaging Beginners in Online {CTF} Competitions for Security Education. In 2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17).
[27] Dunn, M. H., & Merkle, L. D. (2018, February). Assessing the Impact of a National Cybersecurity Competition on Students' Career Interests. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (pp. 62-67).

3.2.3 Funding

National experts inevitably stressed the importance of having appropriate funding to achieve the competition's objectives. This is felt particularly among national organizers who do not receive a regular, medium to long-term budget from their respective governments or in those countries where it is difficult to attracts sponsors, mostly because of the absence of a well-established cyber security industry.

As per the governance structure, a perfect funding arrangement does not exist. The financing model usually depends on the country peculiar situation in terms of economic fundamentals, government's support and private sector sponsorships. However, also in this case there is a convergence towards a mixed/combined model where costs are shared among the key actors that are involved in and benefit from the competition, most notably the government and the private sector. A combined approach is preferable mainly because "a national competition, and a national education program in cybersecurity is profitable for everyone involved" and because "the development of cyber security talent is not solely the responsibility of one of these parties." The obvious benefit of having different sources of funding is to limit the disruption which may occur when the competition's main sponsor stops providing funds and to limit potential disputes between funders who might also be industry competitors.

According to national experts, the EU should be co-sponsoring member states' NCSCs

In the national organizers view, an initial investment by the government is needed to start off on the right foot and "to give the competition a sense of neutrality and importance." Furthermore, according to one interviewee, a national government must support a national cyber security competition "as it is its duty to ensure the future of its young people, to cultivate and utilize their knowledge and skills and to help them in any way it can, so that they can succeed their professional goals."

Being the national competition generally the first step in the creation of national teams that later compete in the ECSC, national organizers feel that the European Union should also co-fund national cyber security competitions: "The European Union, from the beginning of its creation, has as a goal to empower the progress and development of every country that it represents, by cultivating culture and the economy. Therefore, financing a national competition which cultivates and promotes the talents of young people seems as an obligation on the one hand; on the other hand, it seems necessary for member states to share the European Union' knowledge about organizing, conducting and coordinating such a competition."

3.2.4 Public relations and marketing strategy

Organizers emphasize that national cyber security competitions should have a public relations and marketing strategy: it is "very important to assure an overall promotion. (There is) No need to organize a competition when nobody knows about it." According to one interviewee, "public relations are about sending the right messages at the right time, to the right people and creating a dynamic interaction with the general public. A major goal of public affairs is to communicate an event to ensure that it will be covered by the press and to create a presence on the Internet and other media."

A public relations and marketing strategy help achieving multiple purposes. First of all, it is important for the promotion of the event and to reach out to potential participants. It is crucial at the beginning for raising interest among students, but also later when information on the training and the final challenge is released and when it is necessary to keep the interest of students high. This in turn helps achieving another potential objective of the competition, namely, to increase the yearly number of participants and possibly diversify their gender and educational backgrounds. An effective strategy is helpful to reach out to communities of individuals that may have the necessary skills and knowledge to join but are not aware of institutionalized cyber

security competitions. This market strategy is also important to ensure that the event achieves visibility for the sponsors and the rest of the national cyber security ecosystem. As one interviewee acknowledged "a good PA strategy provides visibility to the event and consequently attracts more sponsors. This would allow to provide better resources and even organize better events for the participants." Finally, a communication strategy might also be paramount if a competition was designed to raise cyber security awareness in the general public.

A public relations and marketing strategy is essential to achieve important NCSC's goals, including recruiting participants and give visibility to the event and sponsors

Because a public relations and marketing strategy is useful to achieve different objectives, it should be clearly articulated in order to target the right kind of audience. An interviewee stated that there are at least 5 different groups that such a communication strategy should take into account, namely the public, the industry, the education sector, the (potential) participants and other countries involved in the ECSC. Therefore, "the key to this matter is to know your audience well and be able to identify the appropriate channels to reach them."

A communication strategy is also valuable to build a positive narrative around cyber security as a topic and as a craft, dispelling the myth of hacking as a criminal activity. The strategy would also be important to create a narrative about the competition's success stories, for example when former participants go on to found a company or obtain a highly coveted cyber security job.

As a national cyber security competition usually caters to participants in their schooling age, the communication strategy should directly involve the national ministries of education as well as high schools and universities. A communication strategy should use different tools to achieve its objectives. While it is important to focus on social media to enthuse younger generations, using traditional media such as the TV and radio might be useful to reach a broader audience, especially the older generations as "all these groups need different approaches."

3.2.5 Organization, training and cyber security challenges

National experts think that the initial recruitment should include the largest and most diverse group of individuals in an effort to attract more young talent to cyber security

3.2.5.1 Recruitment and competition's phases

Notwithstanding the possibility of having different approaches based on specific national objectives, organizers tend to agree that the initial recruitment and admission process of a national cyber security competition should include the largest and most diverse group of individuals possible. This is true regardless of whether their countries are able to implement such principle.[28] One organizer stated that his national cyber security competition is open to any individual from 9 to 24 year-old. Furthermore, more than one organizers stress the importance of increasing the participation of females and individuals with an educational background different than computer science: "In the online phase, what we are looking for is the largest number of participants, promoting equal opportunities around the country. Everyone should have the chance to take part." The importance of involving a diverse group of participants has been highlighted in the literature as well [29] [30] [31] [32] [33] namely the ratio of the different genders involved in the competition, their performances in solving different kind of challenges, differences and commonalities in their problem solving approaches and weather a special

[28] Even countries whose objective is to rapidly identify an elite group of students to enter the ECSC competition acknowledge that they would like to include a larger group of individuals at least in the initial phase of the competition, if they had appropriate financial and human resources.
[29] P. Pusey, M. Gondree and Z. Peterson, "The Outcomes of Cybersecurity Competitions and Implications for Underrepresented Populations," in IEEE Security & Privacy, vol. 14, no. 6, pp. 90-95, Nov.-Dec. 2016, doi: 10.1109/MSP.2016.119.
[30] Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: lessons from the launch of the national cyber league. ACM Inroads, 5(1), 53-56
[31] Ricci, M., & Gulick, J. (2017). Cybersecurity Games: Building Tomorrow's Workforce. Journal of Law & Cyber Warfare, 5(2), 183-224.
[32] Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., ... & Hall, L. (2013, June). Cybersecurity, women and minorities: findings and recommendations from a preliminary investigation. In Proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports (pp. 1-14).
[33] Pittman, J. M. (2015, June). Does Competitor Grade Level Influence Perception of Cybersecurity Competition Design Gender Inclusiveness?. In Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research (pp. 49-54).

measure is taken to encourage the participation of diverse groups and participants from non-STEM backgrounds to increase awareness in public.

To do this, national competitions should design a communication campaign that reaches out to potential participants in a timely manner, focusing on schools and being potentially supported by coaches and former alumni to attract newer recruits. Even in the recruitment and admission process "having a public affairs strategy is decisive." When planning the recruitment process, it is important to win the trust of potential participants, which means gaining the acceptance of the local CTF teams and communities that would not normally attend institutionalized national cyber security competitions. One interviewee posits that "finding the best hackers is a nice slogan," but there is a lot of talent who is not attending national cyber competition because "they do not like the word cyber, mainly for its military or governmental connotations."

While it is again recognized that different approaches are possible depending on a country specific objectives, organizers generally think that national cyber security competitions should comprise of at least two phases, namely a national qualifier and a final challenge: "The admission process should involve two phases of selection, which gradually lowers the number of potential participants. The final goal is a small group of elite students." These two main phases may be preceded by an additional admission process with a view to pre-screen candidates, although this would need to be balanced against the objective of creating the largest possible interest in the competition and have the highest possible number of participants at least at the beginning.

NCSCs should have at least two phases: one to recruit participants and teach cyber security knowledge and skills and one to select an elite team of students attending the ECSC

Especially when a longer initial first phase is foreseen, a two-phase competition is considered appropriate as the first part is concerned primarily with teaching cyber security knowledge and skills and raising awareness, while the second part has the objective to identify and choose the participants who are going to be part of the national team attending the ECSC. Regarding the logistics of the two phases, one organizer suggests that "the first selection should be remote; the training phase ideally distributed/remote; and the finals on-site."

3.2.5.2 Cyber security challenges, training and technological infrastructure

The creation of the challenge(s) is also a key factor to ensure the success of a national cyber security competition. This will depend overall on the design and the objectives of the competition, but the types of challenges usually range from jeopardy style, attack-defence and online wargames. Organizers underlined the need to plan the creation process of the challenge well in advance. According to one interviewee, the optimal challenge creation process consists of mainly 4 phases: 1) design/brainstorming phase, when challenge creators produce a rough draft; 2) collaboration/deployment process, when the challenge is deployed in the competition environment; 3) review process, when someone other than the creators attempt to solve the challenge(s) to verify it is solvable; 4) a final phase when the reference solutions are created. Moreover, it is important to create challenges that support the improvement of cyber security skills of all participants: "challenges should be prepared so that everyone is able to enjoy the competition. There should be a wide range of difficulty so that both beginners and proficient players can solve some challenges. Enjoyable competitions are a good advertisement for future events."

The importance to create appropriate challenges according to different skill levels has been found in the literature as well. Researchers [34] [35] [36] [37] [38] investigated participation of individuals in cyber security competitions based on the technical skills they were required to show. Researchers [28,37] investigated whether the difficulty of task performed using specific skills was accurately reflected in the final scoring. Dynamic scoring depends on multiple factors which include the time it took for the task to be completed and how many participants completed it. Based on this variables, the task score changes. Researchers [39] [40] investigated the age group and prior experience of competition participants and how these effect their final ranking in the competition. As different age groups have different competencies level, researchers[41,] investigated how to create balanced challenges for participants and adapt the difficulty level of the competition. In turn, this will motivate beginners to attend and build self-efficacy as they increasingly master cyber security challenges.

Cyber security training should be a core element of a NCSC, improving both cyber security technical proficiency and soft skills

Researchers [42] [43] [44] found that other factors that may motivate people in participating the competition is how the competition is represented. In CTFs, most of the time one can find a scoreboard with very little or no audience engagement. For motivating people, there should be visible and understandable actions going on and a commentary, which can help make sense of things for people with little or no understating of cyber security. This can be used to raise awareness and motivate individuals to participate in similar competitions. National organizers tend to underline the importance of training as one, if not the main, component of a national cyber security competition: “Apart from the participants’ skills, the training is, without doubt, the most important factor for a cyber security competition, since the team is educated to collaborate, practice under pressure and get deeper in cyber security issues.” For another interviewee, training should not be considered as an added value to the competition, but it should be viewed as a core element.

Organizers suggest that “the main purpose of cybersecurity education and any other training program must be to build technical proficiency in their students,” although there is unanimity in considering the training of the so-called “soft skills” (leadership, teamwork, self-learning etc.) as important as teaching them core computer science/cyber security skills. Traditional subjects of training include topics such as software security, cryptography, web security, hardware security etc. At least one organization takes this one step further by designing “the preselection and training challenges taking into account the ECSC Curriculum, NIST-NICE categories, and most demanded skills in the sector,” with the objective of “building tomorrow’s workforce.”

Apart from this common understanding, however, organizers highlighted very different approaches on several key aspects of training, which profoundly shapes not only how the training is designed and delivered, but also how the whole national cyber security competition is conceptualized and its outcomes. It is important to stress that these differences are most of the

[34] Ricci, M., & Gulick, J. (2017). Cybersecurity Games: Building Tomorrow's Workforce. Journal of Law & Cyber Warfare, 5(2), 183-224.
[35] Eagle, C. (2013). Computer security competitions: Expanding educational outcomes. IEEE Security & Privacy, 11(4), 69-71.
[36] Fulton, S., Schweitzer, D., & Dressler, J. (2012, October). What are we teaching in cyber competitions?. In 2012 Frontiers in Education Conference Proceedings (pp. 1-5). IEEE.
[37] Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. IEEE Security & Privacy, 3(5), 27-33.
[38] Gu, Q., Burns, T. J., Rios, S. C., Jordan, T. K., & Underwood, T. (2017, October). An Analysis of Security Competitions for a Beginner's Guide. In Journal of The Colloquium for Information System Security Education (Vol. 5, No. 1, pp. 22-22).
[39] Bashir, M., Lambert, A., Guo, B., Memon, N., & Halevi, T. (2015). Cybersecurity competitions: The human angle. IEEE Security & Privacy, 13(5), 74-79.
[40] Thomas, L. J., Balders, M., Countney, Z., Zhong, C., Yao, J., & Xu, C. (2019, July). Cybersecurity Education: From Beginners to Advanced Players in Cybersecurity Competitions. In 2019 IEEE International Conference on Intelligence and Security Informatics (ISI) (pp. 149-151). IEEE.
[41] Wang, P., & Sbeit, R. (2020). A Comprehensive Mentoring Model for Cybersecurity Education. In 17th International Conference on Information Technology–New Generations (ITNG 2020) (pp. 17-23). Springer, Cham.
[42] Senanayake, R., Porras, P., & Kaehler, J. (2019, July). Revolutionizing the Visual Design of Capture the Flag (CTF) Competitions. In International Conference on Human-Computer Interaction (pp. 339-352). Springer, Cham.
[43] Agada, R., Yan, J., & Xu, W. (2018). A Virtual Animated Commentator Architecture for Cybersecurity Competitions. In Information Technology-New Generations (pp. 43-50). Springer, Cham.
[44] Turner, C., Yan, J., Richards, D., O'Brien, P., Odubiyi, J., & Brown, Q. (2015). LUCID: A visualization and broadcast system for cyber defense competitions. ACM Inroads, 6(2), 70-76.

time enhanced or due by the presence (or lack thereof) of appropriate funding as well as suitable human and technical resources. The main differences concern:

- **Type of training:** This can range from solving challenges online that are permanently accessible and playing CTFs, to more theoretical and conceptual lectures delivered face-to-face. In the middle, there are often combined approaches with a mixture of online training, on site lectures, CTFs and other online gamified activities. The type of training/challenge depends on how the national cyber security competition is conceived. For example, an interviewee pointed out that the difference between permanently accessible online games versus CTFs. In the interviewee's opinion, using online games improves domain specific knowledge as there is usually more time to understand the concepts behind the game; on the other hand, CTFs improve collaboration between participants and communication skills, but they are not necessarily conducive to learning because of the time pressure participants are usually under to solve puzzles.
- **Duration**: The duration of the training/challenge depends again on how the national cyber security competition is conceived. In some countries, the national competition is used only to select participants for the ECSC national team. In this case, the "training" should be considered more like a CTF competition, which may last for as little as 24-48 hours. In other countries, where increasing cyber security knowledge and skills is a top priority, a formalized in-person training may last up to 6 months. Again, in between these two extremes, there are different approaches, ranging from 1 week to some months of training.
- **Target group:** Again, the target group of the training/challenge is chosen depending on how the national cyber security competition is conceived. In some countries, all participants signing up to the national qualifier receive some sort of "training," often in the form of online CTFs that are designed according to different skills levels; in other countries only the participants who win the final challenge who are then selected to form the national team receive training; in the middle, there are different variations which might entail, for example, online training/competition for people signing up to the national qualifier and on-site training for a smaller group of individuals who then attend the ECSC.

There is no agreement among national experts on a standardized cyber security training. National approaches vary greatly depending on NCSC's objectives and resources

Last but not least, national organizers need to make some choices around the kind of technological/technical platform to deliver the training and/or the challenge[45]. To some organizers, the platform choice is crucial when designing the training of the national competition: "the most crucial factor to the national competition's success is the online platform that is used. Such a platform should allow its users to test, train and enhance their penetration testing skills, as well as to exchange ideas and methodologies with other members." The platform should be reliable in order to support the challenge, as well as to be secure so that it is not compromised during the event. It should also offer a good communication tool for participants and organizers. Lastly, it should provide consistent report for the correct assessment, selection and follow up of the participants.

In general, national cyber security competitions have been relying on a variety of technological tools, ranging from self-developed cloud-based platforms to commercially available solutions. Again, this will vary according to the competition's nature, objectives, number of participants but above all the intended goal of the training/challenge. Organizers do not seem to agree on a specific type of infrastructure over another: "This could be a self-developed platform, an open source platform or challenges provided on a server with the solutions sent to an e-mail address." However, some of the requisites are: "online environment with different level

[45] Yamin, M. M., Katt, B., & Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. Computers & Security, 88, 101636.

exercises both attack and defence[46]; (the) skills tested should be related to curriculum[47]; (it should) provide logs as well results; (it should) monitor who is doing the exercise in a "fair" manner." Indeed, at least two interviewees emphasized that the choice of platform is important to incentivize the "right behaviour" and promote development of ethical cyber security practices.

Networking and career fairs can help participants better understand cyber security careers and jobs

3.2.6 Connection with employers and career outcomes

As one of the objectives of a national cyber security competition is to increase interest in cyber security careers, national experts agree that establishing and strengthening relations with employers is a key factor, especially so if it is true that "we do not need hundred thousands of cybersecurity experts, but we need hundred thousands of cybersecurity workers." The importance of cyber security competitions' career outcomes is highlighted in the literature as well. Cyber security competitions are organized not just for personal gratification of individuals and teams but to encourage people to choose cyber security as a career option and reduce the ever-increasing cyber security workforce shortage. According to researchers, providing mentoring and career counselling to participants during the competition will motivate them to choose cyber security as a career path.

Organizers believe that this is achievable by creating a network of people and organizations working in cyber security. This network would make possibilities in cyber security careers more visible and/or make it easier for participants to find internships and other job opportunities after the event. Being part of this network yields clear benefits to employers as well, who are often able to meet and evaluate students who have undergone a rigorous selection process as well as have received relevant training.

Networking events and career fairs are perfect venues for connecting participants with employers. For example, one national cyber security competition runs a "cybersecurity employment and talent forum," which is a meeting point for young talents, future professionals, and the most relevant entities in the field of cybersecurity." It comprises many activities designed to show students what it is like to work in the industry and inspire them to consider a cyber career. It gives students the chance to meet experts, explore potential jobs and educational opportunities and learn about practical next steps. In this forum, actions are taken "to normalize and not mythicize cyber security careers." This shall be done by presenting the different career options and making sure there is support for any student with the skills for a career in cyber security. When connecting to employers, the national competition should inform participants about the different types of cyber security roles available and the career paths leading to those.

Ideally, in the design phase, the national competition should consider what profiles and skills employers are looking for and help them communicate their critical workforce needs and skill shortages. According to one interviewee, "if the communication between learning institutions and companies (employers) is improved, this will lead to a consensus between the needs of the industry and cybersecurity talent."

[46] Yamin, M. M., Katt, B., Torseth, E., Gkioulos, V., & Kowalski, S. J. (2018, September). Make it and break it: An IoT smart home testbed case study. In Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control (pp. 1-6).
[47] Yamin, M. M., & Katt, B. (2019, August). Cyber Security Skill Set Analysis for Common Curricula Development. In Proceedings of the 14th International Conference on Availability, Reliability and Security (pp. 1-8).

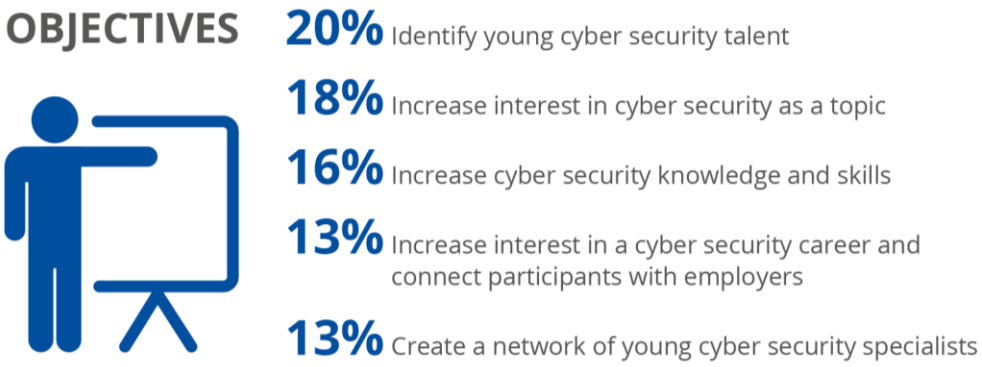
4. CURRENT STATUS OF NATIONAL CYBER SECURITY COMPETITIONS

Based on the key enabling factors in section 3, the researchers created a survey to collect data on these factors and provide a picture on the status of national cyber security competitions in the EU and ECSC partner countries. The survey was sent to the ECSC steering committee on 14th July and closed on 28th August. It was filled by 20 countries out of 22 countries that are listed on the ECSC's website.[48] Given the response rate (90%), the survey provides a reliable indication of the status of national cyber security competitions. The results from the survey are presented below.

4.1 NATIONAL CYBER SECURITY COMPETITION OBJECTIVES

The survey asked national organizers to identify the 4 most important objectives that their national cyber security competition is set to achieve. The graphic below shows what the organizers consider the five most relevant objectives.

Figure 2: Most relevant objectives



Another important objective which however did not make the top five is "raise cyber security awareness" (11%), whereas other objectives such as increase diversity (5%), promote ethics (3%) and modernize the education system (1%) do not seem as popular.

4.2 POLICY RELEVANCE, GOVERNANCE AND PPP

Only 40% (8/20) countries report their national cyber security competitions to be mentioned in or aligned with their national cyber security strategy. Another 40% (8/20) of countries say their competitions are "somewhat" mentioned or aligned. The remaining 20% of countries either are not aligned, or organizers are not aware of it.

In most countries (55%), national cyber security competitions are organized and implemented by a combination of actors. As an example of this arrangement, the ACSC Austria Cyber Security Challenge is organized by Cyber Security Austria (CSA) a private non-profit

[48] https://europeancybersecuritychallenge.eu/#mapcontainer

organization, the Ministry of Defence, the Ministry of Internal Affairs, the Ministry for Digitalization and Economy, the Ministry of Education and the Federal Chancellery, as well as most Austrian universities of applied sciences.

In Belgium, the competition originally started as a private sector initiative with support from the government, but it is now a separate non-profit organization which is in charge and has a strong support from multiple government departments. In 35% of countries, it is either the education sector or an NGO that have a pivotal role in the organization and implementation of the competition. In only 10% of countries this is done by either the government or the private sector only.

Most governments (60%) support cyber security competitions through partnerships and/or collaborations and 20% provide support "somewhat;" 20% of governments do not provide any support. For example, the Cyprus National Team receives funding from the Cyprus Digital Security Authority and the whole competition is promoted to all schools through the Ministry of Education, Culture, Sports and Youth. In 2021, the national competition will be promoted also by the Ministry of Defence to all armed forces. The Digital Security Authority, the Ministry of Defence and the Cyprus Police are part of the competition's advisory board. Moreover, officers from the above organizations participate as mentors.

In more than half of NCSCs, it is a combination of actors that organizes and implements the competition. This is in line with what experts suggest

In Italy, the national cyber security competition is organised by the Cybersecurity National Laboratory who signed strategic agreements with the Security Intelligence Department and the Ministry of Defence. In the Netherlands, the government has a leading part in building and hosting online CTFs to be used during the national competition, which is similar to what happens in Switzerland where the government is an official partner supporting the competition with funding and occasionally with human resources and/or locations for events.

Academia is involved in most countries' national cyber security competitions (65%), providing an array of services and performing multiple tasks. In 25% of countries the education sector is "somewhat" involved. For example, in Estonia, the education sector directly organizes and implements the national cyber security competition. In France, it is responsible to provide training to the students selected to attend the ECSC, which is similar to what happens in Norway, where the Ministry of Justice and Public Security tasked the Norwegian University of Science and Technology to select and train the Norwegian national team for the ECSC.

In Germany, the Cyber Security Challenge Germany (CSCG) has been founded by the Institute for Internet-Security in Gelsenkirchen, which is well connected to the Westfaelische Hochschule, a university of applied sciences in Gelsenkirchen. The CSCG is also connected to several universities to promote the national competition. In Italy, 28 academic institutions (27 public universities and 1 military academy) are in charge of the 3-month long training within the cyber security competition.

Private sector is involved in the vast majority (80%) of national cyber security competitions; in 15% of competitions, the private sector is only "somewhat" involved. In most cases, the main role of the private sector is to provide sponsorships and financial resources. For example, in Cyprus, the private sector participates with mentors (individual volunteers), gives financial support through sponsorships and provides free access to training platforms to the team members and some mentors; they also participate in the National Advisory Board. In Ireland, private companies sponsor the competition, with some providing logistical support and bespoke challenges. In Romania, the private sector supports the competition with financial, technical, and human resources.

4.3 FUNDING

The survey asked national organizers to state the overall budget of their national cyber security competition, but only 12 out of 20 countries provided estimates. Although it is unclear to what extent the Covid-19 health emergency had an impact on these figures, the (total budget estimate for these 12 national cyber security competitions is €733.000. If one dismisses the highest and the lowest amounts, the average budget for 10 competition is approximately €37.000.

In this context, only 25% of national cyber security competitions declare to have enough financial resources to achieve the competition's objectives. Most competitions (40%) state to have "somewhat" enough resources while 30% say to not have enough resources.

The survey also asked what activities would be implemented if more resources were made available. The four most mentioned activities are:

- Further development and provision of cyber security training, including quantity and quality of challenges, but also training platforms and trainers;
- Increase in the number of students attending the competition, including larger on-site events;
- Support ECSC's travel and accommodation costs;
- Promotion, communication and awareness raising activities.

There are several activities that NCSCs would improve if they received more financial resources, including further developing their cyber security training

Most (65%) national cyber security competitions are funded through a combination of sources. The most popular formula is usually a combination of resources coming from the government and the private sector, although it is not unusual to have the education sector and/or some NGOs contributing to the budget. Overall, from the limited data provided by countries, it seems that when the competition is funded by a combination of actors, the private sector is the one contributing the most. For example, in Switzerland the national completion organizer receives their funding from a combination of government, private sector and a philanthropic entity. They also organize side events like cyber security conferences during the completion and sale tickets' events for funding.

Only 35% of national cyber security competitions rely on a single source of funding: 25% rely on only government funds and 10% rely on private sector resources. Interestingly, one country mentioned that it is planning on shifting from a funding model based exclusively on government support to a financial model based entirely on private sector sponsoring.

Most national organizers (80%) believe that the EU should fund national cyber security competitions and 53% of them believe the EU should cover at least 40% of national cyber security competitions total costs. They provide several reasons why this should be the case. According to one organizer, "the ECSC is a European event that can be a force multiplier for Europe by building both formal and informal networks of cyber security specialists. This is of value for both EU as a whole and for each nation." By supporting national cyber security competition, the EU would invest in a more resilient cyber future for Europe. For another organizer, by already funding its own competition, a country shows its commitment to make a national challenge part of the country's cyber security capacity building effort and EU co-sponsorship would contribute to this objective. This would be useful as "a part of a pan-European action/plan. It would encourage more collaboration, more integration, more networking and a closer working relationship between states." Moreover, in countries where cyber security is not considered a priority, EU co-funding would help raise the attention on the topic. Finally, in a post Covid-19 era, it is possible that resources will be redirected towards other sectors and tasks, despite the importance of educational cyber security activities.

4.4 PUBLIC RELATIONS AND MARKETING STRATEGY

Most national (60%, 12/20) cyber security competitions have a communication and public affairs strategy; 40% of competitions claim to have "somewhat" of a strategy. For example, in Austria, the communication strategy addresses 4 main target groups: public and private sectors, academia (teachers and professors), potential participants (students from 14 up to 30 years-old) and mass media (primarily online media).

In Germany, the national competition is working together with some news outlets like heise.de and golem.de, which are well known it-news pages in Germany. The competition is also working together with an influencer with 500.000+ follower on YouTube. In Italy, the communication of the national cybersecurity competition is managed by a specialist social media manager and journalists in charge of public affairs and communication management.

In Poland, there is a communication plan which describes: a) target audience, i.e. universities and faculties from which potential participants come from; b) social media, blogs, news websites that should know about the competition; c) schedule and content of the information the competition provides before it takes place. In Spain, INCIBE, the organization in charge of organizing the Spanish national cyber security competition, has been building strong visibility on traditional and social media channels during and after the event last year.

Almost half of national competitions (45%) have an audience engagement platform, while another 45% do not have any; for 10% of competition is unknown whether they have it or not as indicated . For example, in Belgium, there are announcements and there is a scoreboard, but this is more aimed towards participants and not for the public. In Germany, there is an official scoreboard for the online qualification as well as the finals. In Ireland, the competition actively uses use social media, especially Twitter, for updates and engagement and it is planned to have a commentator on site to give updates.

In the Netherlands, there is a live streaming throughout the day with interviews with organizations, sponsors and jury. Rankings are shown during competition as well as the final results. In Spain, there is speaker who encourages the participants and audience during the finals, but there is no engagement platform in the online rounds.

4.5 ORGANIZATION, TRAINING AND CYBER SECURITY CHALLENGES

4.5.1 Recruitment and phases of the competition

The survey asked how many people signed up to the initial admission phase/round of the latest edition of national cyber security competitions and how many are "active" users. Results are provided Table 2:

Table 2: Number of participants in national cyber security competitions

Country	Signups	Active users
Austria	600	250 (40 “very” active)
Cyprus	157	65
Czech Republic	Over 5.000	From 3.000 to 4.500
Estonia	300	100
France	2.000	-
Germany	770 (junior and senior category) 1068 (open competition)	200 (junior and senior category
Greece	50	-
Ireland	300	-
Italy	4.452	518
Malta	20	-
Netherlands	145	145
Norway	158	55
Poland	77	38 (solved at least one challenge)
Portugal	42	-
Romania	500	250
Spain	1.792	168
Switzerland	1.000	200-100
Total	**17.363*** (*17 countries)	**1.989*** (*11 countries)

There are big differences in the ability of countries to recruit participants and keep them active throughout a NCSC

Overall, the 17 national cyber security competitions providing data totalled 17.363 signups; of these, 1.989 were “active” users although it is important to notice this figure is the result of data provided by only 11 countries only (Table 2).

There is a variety of means, instruments and targets that national cyber security competitions use to recruit students to attend their activities and, most of the time, the recruitment is part of a larger communication and public affairs campaign. As the competition is geared towards students, collaboration with the education sector (mostly higher education and secondary schools) and use of social media are widely spread. Some competitions also rely on their network of former contestants and word of mouth.

For example, in the Czech Republic, dissemination activities to encourage participation are done through different channels and using different approaches: 1) Direct contacts with schools and their students; 2) via founders and owners of the schools including government and regional government institutions; 3) Through former competition participants, their friends and contacts 4) via NGO with focus on ICT teacher, English language teachers, etc. 5) Using social media and national media (TV, radio) etc.

In Estonia, there is a direct communication channel with schools, which sometimes allow to organize promotional events inside classrooms. Communications are also sent to university students through university mailing lists. Another strategy is to look for networks of young talents and gaining access to them in order to supply relevant information about the competition. Finally, information about relevant activities are sent also to those who already have attended previous events.

In the Netherlands, in addition to schools and universities, the national competition also reaches out to student organizations and NGOs that support young hackers. Last year's ECSC team members played an important role in reaching out to potential participants.

In Poland, dissemination activities are done mostly through social media and local CTF teams.

In Portugal, the national competition is open to all levels of education (school pupils and university students), therefore the dissemination is made through school, universities and Internet (websites and mainly social networks).

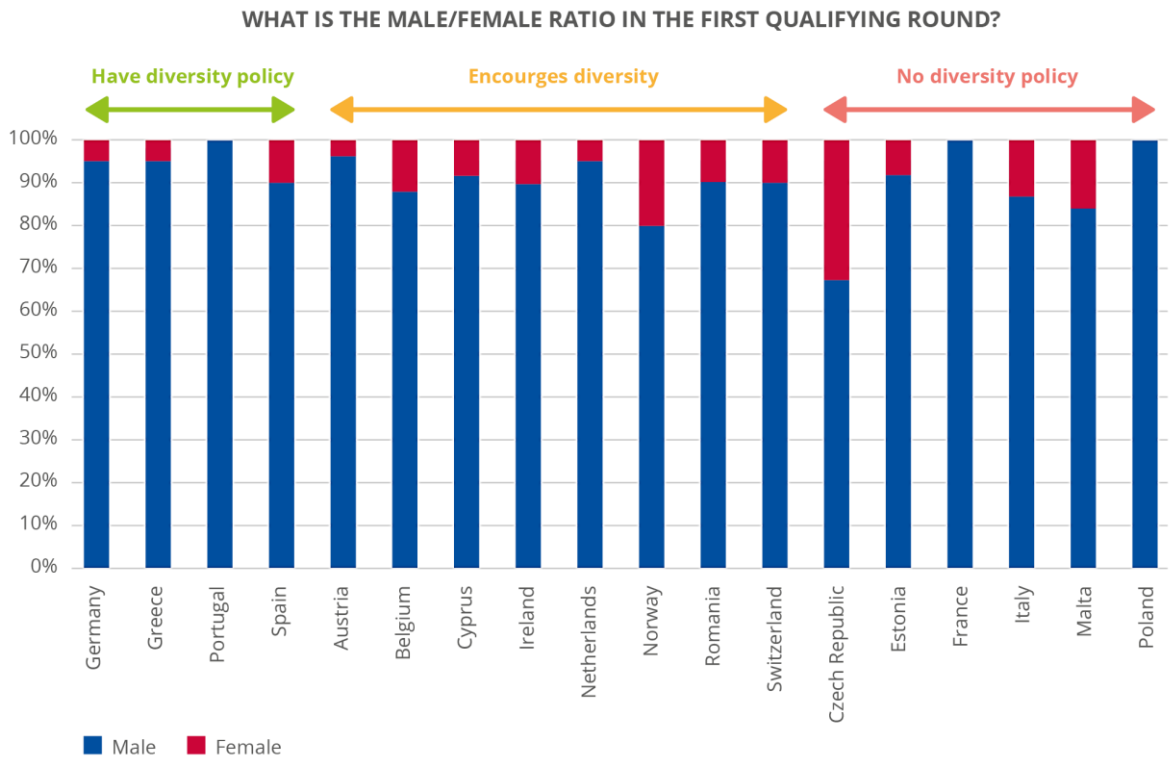
The survey asked what pre-existing knowledge and skills participants need to possess to be able to participate in the first admission round. National cyber security competitions require:

- Cyber security (10%)
- Math (15%)
- Basic computer science skills such as web searches and the Office suite (25%)
- Intermediate to advanced computer science such as programming (20%)
- A combination of the above (30%)

With the exception of the Czech Republic, most NCSCs tend to have a low representation of females

Qualitative data show that when national cyber security competitions require a combination of pre-existing skills most of the time it means that students are initially asked to solve easier challenges, but then the expertise level required to advance quickly increases. As one organizer describes one “can start without any pre-existing knowledge but the chance to reach top ranks or mastering the qualifying for the final are not too high - so we recommend having basic network and scripting skills as well as basic cybersecurity skills (early red-teaming).”

Figure 3: Diversity in national cyber security competitions



National cyber security competitions are mainly attended by male participants. Organizers often report to have only between 5%-10% or lower of female participants attending the first qualifying round as indicated in Figure 2, with this percentage usually dropping even further in the final rounds of the competition.

An exception is the Czech Republic, where the percentage of female contestants in the first qualifying round has been "above average" compared to the rest of national cyber security competitions and on the rise since 2016:

Table 2: Percentage of female contestants in the first qualifying

2016	2017	2018	2019
27%	29%	32%	33%

Against this background, 35% of national cyber security competitions do not have a specific policy with the aim to increase the gender and education diversity of its participants, while 25% state to have one; 40% of competitions declare to have a specific diversity plan "somewhat". The result of the survey question about promoting gender diversity through specific polices is presented in figure 2.

For example, in Austria a greater participation is encouraged by promoting role models. In Belgium, the national competition works with various female cyber security professionals and other organizations to try to motivate more girls to participate and provide some coaching. In Norway, the national competition reaches out to potential female participants through existing organisations and networks that work on recruiting females to study STEM subjects In Spain, the national competition employs a combination of elements, including a public affairs strategy that targets kids at a young age, and engages with female role models to motivate young women to take part in technical careers.

Only 25% of national cyber security competitions keep involving the participants who do not make to the final round; 25% of competitions declare to keep involving them "somewhat," while 35% of them do not involve them in further activities. There are different ways that national competitions use to involve the participants who do not qualify, even though the evidence provided by survey results is scarce. For example, in Belgium the challenge writeups are shared by creators to allow all participants to learn as well and not just the participants who have to tackle them in the final round In the Czech Republic, the competition includes an educational component, which engaged over 10.000 in 2019 (but only 3000 in 2020 due to the Covid-19 health emergency).

In Italy, the national cyber security competition started the OpenCyberChallenge.IT (OCCIT) programme in 2020. The OCCIT was open to participants who were not admitted to the cyber security training at the local university and the local/national challenge. Through this programme, participants had the possibility to access cyber security online lectures, crash courses and challenges.[49] Approximately 1.300 students were invited to enrol and 511 accessed it. In Germany and the Netherlands, the competitions foresee a Discord channel where participants can interact.

The survey also asked details about the "admission process" of national cyber security competitions. National cyber security competitions are generally based on one or multiple qualifying rounds/phases, where participants compete against each other in solving cyber

[49] https://cybersecnatlab.it/open-cyberchallengeit-programma-formazione-esteso-nuove-leve/

security challenges, and a final challenge. These qualifying rounds are usually online. It can be argued that the biggest difference among countries lies in the length and number of qualifying rounds. During this initial qualifying round, the best contestants are selected depending on their scores (i.e. number of challenges solved, but also interview performance in certain countries) and are usually invited to attend a final national challenge/CTF. The final national challenge usually takes place on-site (except for 2020 competitions due to the Covid-19 health emergency). There are some variations to this model, for example when a formal training period is incorporated as an integral component of the competition before a national final challenge.

France is an example of competition with a "short" single-phase admission plus a final challenge. There, an "open admission challenges platform" is open for two weeks, where everyone can participate and try to solve the 20 CTFs in the platform. Then, the best 30 candidates are selected for the final bout, which lasts for a full day. There are about 10 challenges and the best 5 junior and 5 senior players are selected to form the French national team.

Germany and Austria are examples of competitions with a "long" single-phase admission and a final challenge. The German national competition foresees an online three-month long qualification round. After this, 20 participants are invited for an on-site final event. A long qualification phase from May to September (4-5 months) is also foreseen in the Austrian competition. In this phase, the competition consists of 12 remote challenges,. The best 10 juniors and 10 seniors are then invited to compete in the ACSC final in November. The best candidates (both juniors and seniors) are then invited to the ACSC centre of excellence where they are supported beyond the challenge in their cyber security carriers.

There are several approaches regarding the number and length of phases that a NCSC should have

Switzerland is an example of competition with a "permanent" single-phase admission plus a final challenge. There, a challenge platform is open all-year-round, where beginners, intermediate and expert level contestants can find challenges in their respective sections. Those reaching expert level by collecting enough points qualify for the final round. To maintain expert status, these contestants must remain active each year (i.e., solving a challenge or sending in a new challenge etc.). In the final round, the best candidates are selected for the ECSC team.

The Czech Republic is an example of competition with a multi-phase admission plus a final challenge. This competition consists of two rounds and a final: 1) qualification round, which is accessed by approximately 400.000 students each year; 2) second round, which is accessed by 2000-1000 students and 3) a final round, which is accessed by 50-40 students. From this smaller group, there is another screening process involving two bootcamps, where 15 students are selected to form the Czech national team.

The Netherlands and Italy are examples of competitions integrating a formal training period before the final challenge. In the Netherlands, after the national competition round (phase 1), there is a bootcamp/training week involving 22 participants, the best achievers of phase 1 in addition to two "wild cards." Then, the competition foresees a final event where 10 players are selected for the national team. The Italian competition comprises a first qualifying round which is divided in three tests (an online pre-test and two onsite tests, involving logic and programming quizzes). In 2020, 4.452 students signed up online and 560 students advanced from the qualifying round to the next phase. The following phase is a formal training taking place in 28 universities and centres across Italy lasting for approximately 3 months. At the end of the training period, participants attend local cyber challenges, which usually further decrease by approximately 70% the number of candidates who later attend the national final. In the final challenge, the best contestants are then selected to form Team Italy.

4.5.2 Cyber security challenges, training and technological infrastructure

The survey also asked the type of challenges that are included in the competition. There is a great variety of cyber security topics and skills that competitions use. Very few competitions seem to be teaching non-computer science topics such as cyber security law and policy, ethics and/or data protection. Those that are most often mentioned are:

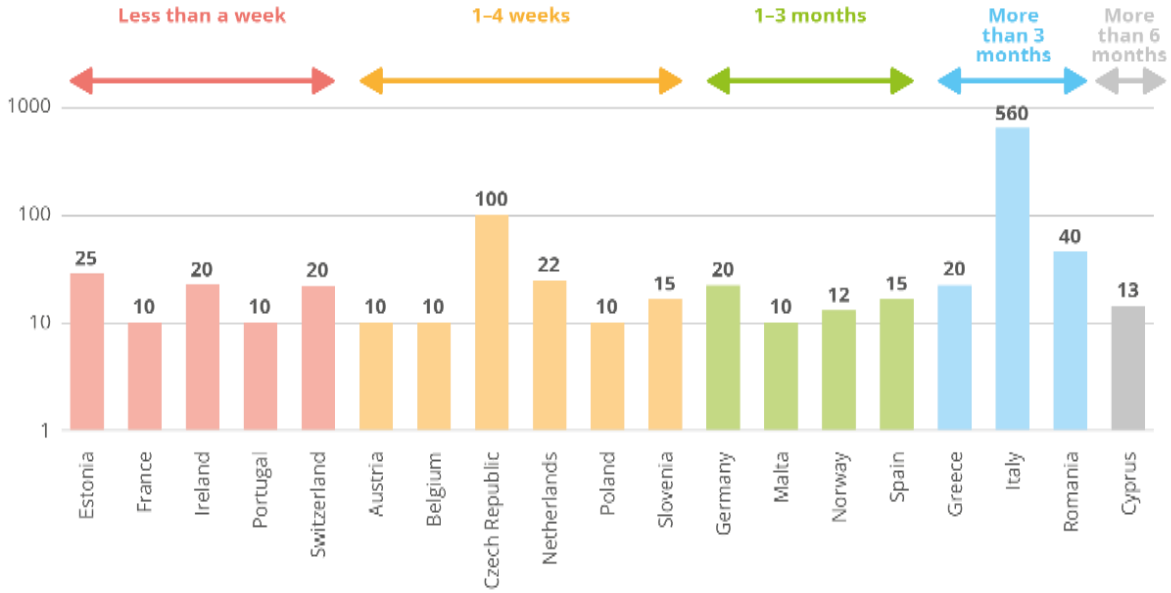
- Forensics
- Cryptography
- Incident response
- Cracking and reversing binaries
- Threats and vulnerabilities
- Social engineering
- Attack/defence tactics
- Pwning and reverse engineering
- Web security
- Binary exploitation and mobile apps exploitation

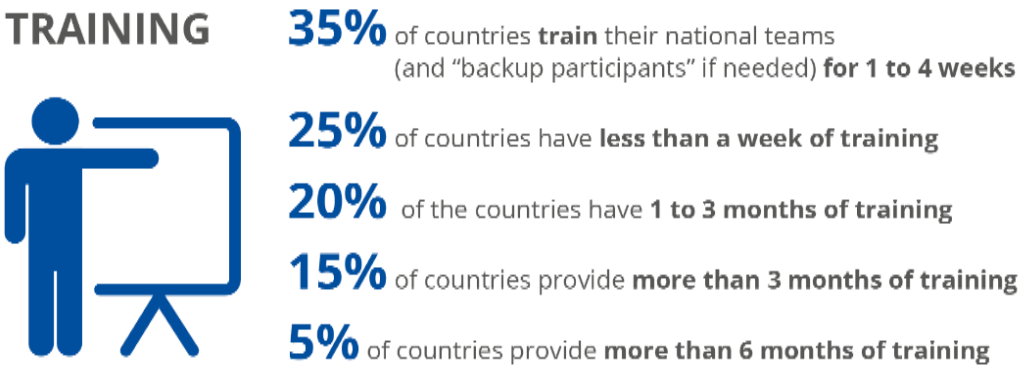
Interestingly, in Belgium, there are challenges put forward by the competition's sponsors. All major sponsors provide a challenge relevant to how they use cyber security, which "can range from theoretically finding a backdoor in one of the companies' products, to working with a threat intel platform or role-playing an incident response process."

In Spain, challenges/categories are defined considering ECSC Curricula, NIST-NICE categories, and skills most in-demand in the labour market. In Norway, the challenges in the qualifying round are based on the ECSC curricula. In preparation to the ECSC, almost every country (90%) organizes extensive special training sessions for participants, while two countries Ireland and Poland organize team meetups before the competition. Countries have different training methodologies, especially regarding the training length and the number of participants trained (Figure 4):

- 35% of countries train their national teams (and "backup participants" if needed) for 1 to 4 weeks
- 25% of countries have less than a week of training
- 20% of the countries have 1 to 3 months of training
- 15% of countries provide more than 3 months of training
- 5% of countries provide more than 6 months of training

Figure 4: Training provided by national completion organizer with respect to time and number of participants trained for ECSC





In terms of the number of trained participants, Czech Republic and Italy are an exception as they train a larger number of individuals than most countries. When qualitative data were analyzed, it was found that the Czech Republic trains a wide range of individuals, from school children to university students, thus having a larger portion of the student's population covered. In Italy, several education institutions signup to train at least 20 individuals for 3 months. The trained individuals then compete in a national final for the selection of national team.

Half of the countries (50%) also teach non-technical skills in their training like teamwork and collaboration, leadership, presentation, stress management, writing, etc.; 40% of countries include non-technical skill in their training programs "somewhat," while10% declared to have no information about the non-technical skills are taught in their training programs . Belgium and the Czech Republic use social activities to teach these skills, while Italy uses game-based skill teaching and assessment; Malta uses mockup presentations for certain tasks. Romania, Spain and Slovenia teach these skills within their overall training programs for national teams.

Austria, Cyprus, Estonia, Ireland, Poland and Norway reported that they "somewhat" teach soft skills in their trainings. Austria uses a single day before the final to teach presentation skills;

Countries generally organize cyber security training as a part of their NCSCs, but the length and target of these trainings vary vastly among them

Estonia provides social activities to participants for team building. Ireland and Cyprus have identified the importance of such skills and are working to integrate them in their training program. Poland discusses previous CTF writeups as a team to share experience from previous challenges. Finally, Norway uses training weekends as team building events where the focus is on building teamwork and trust among the participants.

Most countries (60%) use online platforms to train participants. Some of them (Austria, Cyprus, Ireland, Norway, Portugal, Romania, Spain, Switzerland) use public commercial platforms, (Table 3). Belgium, Germany, Italy, Czech Republic, and Poland use proprietary and self-developed platforms for online qualification and training. Estonia outsources the development of qualification and training challenges to private companies every year. Instead, 15% of countries (Netherlands, France and Malta) don't use any online platform, but they provide onsite training.

Table 3: Platforms used to provide training and challenges

No.	Name	Training Platform
1	Austria	hacking-lab-ctf.com
2	Cyprus	hackthebox.eu, tryhackme.com, icsi.co.uk
3	Ireland	github.com/CTFd
4	Norway	hackthebox.eu
5	Portugal	github.com/CTFd
6	Romania	CyberEDU.ro
7	Spain	ihacklabs.com
8	Switzerland	scs.hacking-lab.com

National teams that attend the ECSC are usually formed by a combination of junior and senior players, which tend to have different levels of cyber security understanding and skills. Therefore, national cyber security competitions should have balanced challenges so that each participant is challenged with cyber security games at its own level.

Austria, Belgium, Cyprus, Greece, Ireland, Malta, Netherlands, Portugal and Switzerland include in their national cyber security competitions challenges with different difficult levels, (easy, medium and hard) to accommodate participants with different skill levels. In the Netherlands, more difficult challenges are left for the top players. Switzerland has defined difficulty levels with corresponding challenges and the selection of the right level is done by the participants when they join the platform and are evaluated based upon their overall performance.

Italy, Romania and the Czech Republic specifically align and adjust the competition's difficulty level and include challenges with increasing difficulty level each year. They have a feedback mechanism whereby they take onboard the input of previous years' participants based on an assessment of their knowledge and skills, and develop new challenges based upon this assessment. Poland uses dynamic scoring for assessing the difficulty of challenges as well as participants' feedbacks.

In France, the competition organizers make some challenges deliberately easy to encourage the participation of juniors, which is similar to what happens in Germany, where organizers make special tutorials for juniors to ensure that beginners have at least the chance solve some

easy challenges. Finally, Spain uses a threefold approach. First, they consider participants age and experience before designing the competition. Second, they develop competitions that are not linear, whereby participants can explore different challenge categories in which their knowledge and skills can be assessed based upon their performance. Finally, they conduct awareness raising sessions for juniors in schools with the goal to inspire them to join the cyber security sector by providing necessary educational tools that are required for cyber security.

Conducting cyber security competitions requires a lot of technical capabilities, including setting up the necessary infrastructure, defining evaluation and monitoring mechanisms. [50] The survey asked participating countries whether they have sufficient capabilities to conduct such competitions and whether are willing to assist other countries that do not possess such capabilities: 29% reported that they have sufficient capabilities and are willing to provide assistance to other countries; 57% stated that they have sufficient capabilities but are not able to help due to administrative and time constrains; 14% stated that they do not have the required technical capabilities.

40% of NCSCs have limited or no activities in which their participants are linked with employers

4.6 CONNECTION WITH EMPLOYERS AND CAREER OUTCOMES

One of the main objectives of national cyber security competitions and the ECSC is to identify young cyber talent and to increase interest in a cyber security career among young people. Most of the participating countries recognized the importance of achieving such objective and attempt to actively engage participants with potential employers: 60% of national competitions have already integrated participants-employers engagement platforms, while 20% have some sort of informal engagements; only 20% do not have any kind of engagement.

For example, Germany and Czech Republic organize special recruiting fairs for competition participants, while Austria, Belgium, Cyprus, and Ireland actively involve sponsors to provide job opportunities in the competition. In Romania, training to the national team is provided by the private sector with the possibility for trainees to get hired at the end of it. In Malta, the national cyber security competition offers placements as a summer job to participants.

Two countries that are concretely focusing on the employability of their competition's participants are Italy and Spain. In Italy, all participants' CVs are made available to the private sector sponsors of the competition via a custom-made platform. In addition, after each on-site competition a recruitment fair is organized, involving both public and private sector actors. In Spain, the main goal of the competition is to identify, attract, train, recruit, and place the next generation of cybersecurity professionals and the national competition achieves this by organizing the "Cybersecurity Employment and Talent Forum," which is designed to show participants what it is like to work in the industry and inspire them to consider a cyber career.

Countries like Estonia, Norway, Switzerland, and other countries have not integrated this concept in their competition yet, but they organize networking events like conferences and workshops with public and private sector actors to provide competition participants with opportunities to engage with potential employers. In the Netherlands, the private sector organizes some events, no employers-participants engagement especially designed to increase job opportunities is present at the moment. Similarly, Poland has not established a direct link between participants and employers, although some former participants were hired by the national CERT. Portugal is planning on starting to develop a participants-employers connection in the future.

[50] National Exercise - Good Practice Guide. (2016, February). Retrieved November 15, 2020, from https://www.enisa.europa.eu/publications/national-exercise-good-practice-guide

Alumni networks could provide newcomers insights into a new field and sector, which might help them navigate complex skills development and career choices like those that cyber security presents. Hence, the survey asked whether national competitions have established alumni networks to help with this aspect: half of competitions (50%) have already such networks in place, whereas 40% of national competitions have not.

Countries like Estonia, Austria, Czech Republic, and Romania actively engage former competition participants in the organization of the competition, coaching and advertisement campaigns. Cyprus have mentors that provide guidance to newcomers. Germany encourages former participants to join their nonprofit organization as members. Greece and Ireland have alumni networks, while Malta and Netherlands organize social gatherings between former participants, the private and the public sectors to share different ideas and opportunities.

A formal alumni network does not exist in countries like, Belgium France, Italy, Norway, Poland, Portugal, Spain, and Switzerland, although Belgium and Switzerland report the existence of informal settings populated by some competition participants. Norway is currently working on the development of such a network.

As stated earlier one of the main objectives of national competitions is to identify young cyber talent and to promote cyber security as a career choice for young people. Against this backdrop, the carrier progression of former participants can provide key insights on cyber security and career development of young specialists. Hence, the survey asked whether national competitions collect data about the career choices of former participants.

Most countries (55%) do not collect such data, while 20% do; and 15% “somewhat” collect such data. Romania, Switzerland, and the Czech Republic remain in contact with former participants who supply information about their career progression. Austria, Spain, Greece and Estonia collect such data, but did not provide further details on how this is done. They use this data for sharing career opportunities as well as training and coaching purposes.

5. OPPORTUNITIES AND CHALLENGES FOR A COMMON ECSC ROADMAP

This chapter provides an analysis of the survey results (section 4) while considering the identification of key factors as outlined in section 3. The aim of this chapter is to provide tangible elements for the establishment of a common ECSC Roadmap (section 5).

5.1 NATIONAL CYBER SECURITY COMPETITION OBJECTIVES

Results show a certain consensus among organizers about the 5 main objectives that a national cyber security competition should have, namely:

- Identifying young cyber security talent
- Increasing interest in cyber security as a topic
- Increasing cyber security knowledge and skills
- Increasing interest in a cyber security career and connect participants with employers
- Creating a network of young cyber security specialist

Results are in line with what found in section 3 and aligned with ENISA recommendations for the ECSC [25], except for the objective “to create a network of young cyber security specialists.” This objective did not strongly emerge in section 3 and it is overall considered more important than “raise cyber security awareness,” which instead was regarded as highly important during interviews with some national organizers.

According to the survey results, identifying young cyber security talent and increase interest in cyber security topics are the most important objectives a NCSC should reach

Considering the results of the survey, it can be argued that a common ECSC roadmap should be based on these five main objectives. Whether resources should be distributed according to the ranking provided by the survey is an aspect that countries should reflect upon.

It is interesting to note that, despite the cyber security skills shortage being a policy problem frequently mentioned as a rationale behind the establishment of national cyber security competitions, increasing interest in a cyber security career is ranked only as the fourth objective. The authors of this report wonder whether this objective should deserve more attention in the organization and implementation of national cyber security competitions, if countries consider the shortage of cyber security professionals a serious issue that cyber security competitions could tackle. Similarly, and still against the same background, perhaps a common ECSC roadmap should also reflect whether the objective “increasing the number of participants” should be also formalized and given more attention vis-à-vis other objectives.

5.2 POLICY RELEVANCE, GOVERNANCE AND PPP

A common ECSC roadmap should make sure national cyber security competitions are more "policy relevant" as only 40% of competitions are mentioned in countries' national cyber security strategies. Although not all national organizers consider it desirable, it is generally considered valuable for a national cyber security competition to be regarded as a national instrument enabling a better national cyber security posture. Competitions that are "on the policy radar" are, according to organizers, more likely to gain credibility, have a bigger impact and might obtain financial resources more easily. Make cyber security competitions more "policy relevant" would also have the welcomed consequence to make countries more aware of the need to have a more systematic policy and vision on cyber security education. If it is agreed that the lack of cyber security professionals is an important issue as, for example, the lack of coordination in case of a cyber-crisis, then policies in the realm of cyber security education – such as national cyber security competitions – should have the same level of attention that other cyber security policies receive.

There should be a recognition of the importance of NCSCs in achieving countries' cyber security objectives when it comes to cyber security education and skills

The survey found that in 55% of countries it is a combination of actors that organizes and implements a national cyber security competition. This in line with what found in section 3 and what suggested by ENISA [51] [52], which posit that, despite the absence of a universal governance structure, a public-private partnership involving the key actors of a national cyber security ecosystem is usually considered a favourable governance solution for a national cyber security competition. As 45% of national competitions are reported to be organized and implemented by only one organization/actor, a common ECSC roadmap should encourage more countries to involve more actors in national cyber security competitions and reap the benefits of a PPP.

The survey found that governments support cyber security competitions through partnerships and/or collaborations in most countries (60%), whereas governments provides a more limited or no contribution in 40% of countries. Section 3 found that government's support is essential, especially when national competitions are in their "start-up phase," which nowadays seems to be the case for many competitions in the EU and ECSC partner countries. Because of these findings, a common ECSC should encourage governments to more firmly support national cyber security competitions, especially when these are newly established and when the rest of the national cyber security ecosystem cannot adequately support them. This is especially true given that academia (65%) and the private sector (80%) seem to be overall more involved in national cyber security competitions than governments (60%).

[51] Cyber security competitions — the status in Europe (2014, October). Retrieved November 15, 2020, from https://www.enisa.europa.eu/publications/cybersecurity-competitions-2014-the-status-in-europe
[52] The European Cyber Security Challenge: Lessons Learned report (2017, December). Retrieved November 15, 2020, from https://www.enisa.europa.eu/publications/the-european-cyber-security-challenge-lessons-learned-report/at_download/fullReport

5.3 FUNDING

Section 3 found that appropriate funding is one of the key factors enabling the success of a national cyber security competition. Only 12 out of 20 countries provided estimates regarding the cost of their national cyber security competitions and, based on these, the survey found that on average national cyber security competitions have a budget of approximately €37.000.

However, this average should be contextualized and taken with great caution. First, it is unclear to what extent the Covid-19 health emergency had an impact on the costs provided in the survey. For example, it is possible for this estimate to be on the lower end of the spectrum given that the health emergency has moved many activities online, therefore decreasing the costs of certain events which would normally be on-site and face-to-face and thus generally more expansive. Secondly, and most importantly, costs vary according to the nature of the competition. In this regard, it is impossible to not notice that only one country accounts for 49% of the total budget, out of the 12 countries who provided data, which is due to the fact that the country in question provides a "long" training to a large number of participants. To generalize from this example, the budget of a competition which provides a 6-month training to over 1.000 students with a mix of instruments (online and face-to-face) will clearly cost more than a competition which does not provide any training and only foresees a 48-hour CTF. This example reveals that the there is no "one size fits all budget" and this will ultimately vary according to the nature and the ambition of the competition. This means that if a "common ECSC Roadmap budget" was to be established, it is possible that the estimate would change, depending on the level of ambition that this common ECSC Roadmap would have, especially in terms of number of participants involved, length of training, type and quality of challenges provided etc.

Appropriate funding is key for the long-term sustainability of NCSCs. National governments and the EU should consider increasing their financial support to NCSCs

Against this background, survey results show that only 25% of countries state to have enough financial resources to achieve their objectives. Moreover, if more resources were available, national competitions would use them to deliver core activities such as more cyber security training, increasing participants' attendance and paying for travel and accommodation costs related to the ECSC competition and communication activities. These are important activities which, if enhanced, would make national cyber security competitions likely more successful. It comes as no surprise then that most national organizers (80%) think that the EU should co-fund cyber security competitions, with 53% of national organizers believing that the EU should sponsor at least 40% of national cyber security competitions total costs.

Against this backdrop, a common ECSC Roadmap should:

a) make sure national competitions have appropriate financial resources to meet their current objectives;
b) encourage the 35% of countries who receive funding from a single source to attempt to diversify the sources of their budget, when this is feasible and practical;
c) consider whether governments and the EU should increase their financial support to further develop national cyber security competitions. We believe that an increased governmental and EU support would have several benefits, including: 1) making the establishment and implementation of competitions more stable, allowing national organizers to focus on medium-to-long term goals rather than having to fundraise; 2) diversifying the origins of funding, especially if the economic crisis induced by the Covid-19 pandemic would reduce financial resources that are usually made available by other actors; 3) helping competitions gaining more prestige and credibility in the eyes of their stakeholders.
d) encourage national competitions to follow ENISA's recommendations [48] in overcoming funding issues by pitching attractive sponsorship scheme to the private sector, engaging with governments by highlighting the strategic importance of national competitions leading to the ECSC, and setting entry fees for side events during the competitions like conferences or job fairs.

5.4 PUBLIC RELATIONS AND MARKETING STRATEGY

Most national cyber security competitions (60%) reported to have a communication and public affairs strategy. Section 3 found that such a strategy is essential to ensure an overall promotion of the event in order to reach out to potential participants, raise interest and help the event to achieve visibility for the sponsors and the rest of the national cyber security ecosystem. Moreover, such strategy is also fundamental to create a positive narrative around cyber security and to promote the competition's success stories. To increase awareness, ENISA highlighted the importance of a media strategy for cyber security competitions and encouraged them to leverage the possibilities that are offered by social media.[53]

Additionally, engaging the audience during the competition in an interactive manner using commentary and different competition visualization techniques other than scoreboards will help in increasing public awareness about cyber security.

While most of national cyber security competitions report to have a communication and public affairs strategy, a common ECSC roadmap should encourage the 40% of national competitions who said to have it "somewhat" adopted to develop a fully-fledged communication plan, when resources are available. Given the importance of such a strategy to achieve multiple vital objectives, a common ECSC Roadmap could benefit from an enhanced coordination of competition's public affairs and marketing campaigns with the support of ENISA's public affairs team and activities. Moreover, additional research could be done to create a repository of best practices which could be accessed by those countries who have not had so far the resources or the know-how to put in place wide-ranging communication campaigns.

5.5 ORGANIZATION, TRAINING AND CYBER SECURITY CHALLENGES

5.5.1 Recruitment and phases of the competition

Section 3 advanced that a national cyber security competition should involve the largest and most diverse group of people, at least at the beginning of the competition. The purpose of involving a larger group of individuals would be to expand the pool from which to select the team attending the ECSC, but also to increase interest in cyber security and its careers in a larger group of young people in the context of the cyber security skills shortage.

It is estimated that NCSCs across Europe involve almost 22.000 students and 3.500 of them are active

Based on data provided by 16 countries in the survey, national competitions totalled slightly more than 17.000 signups. Therefore, it estimated that the 20 national cyber security competitions who took part to the survey could potentially involve almost 22.000 students, of whom approximately 3,500 could be "active users."

As for the funding, this estimate should be put in context. In fact, out of the approximately 17.000 signups totalled by 16 national competitions 66% come from only 3 countries (Czech Republic, France and Italy). Similarly, out of the approximately 2.000 active users totalled by 11 national competitions, 51% are active users from only 3 national competitions (Austria, Italy and Romania). Participation data varies greatly among countries and some national cyber security competitions like those in Italy, Spain, France, Germany, Switzerland and Czech Republic were able to sign up thousands of participants,while other countries struggled to do so (Table 1).

Hence, a common ECSC Roadmap should set guidelines on how to assist countries that are currently struggling to attract a higher number of participants. Multiple factors such as budget, government support and media strategy likely affect the number of participants that are initially involved in the competition so suggesting only one solution to this issue would mean not understanding its complexity and the multiple elements that influence it. However, a reasonable initial measure could be to involve the education sector and the ministry of education in

[53] This was analysed by the impact of social media reach of ECSC of 2017 and 2018 which was 199 913 and 5 062 457 respectively for hashtag #ECSC20XX.

spreading information related to the national cyber security competition, given the fact that in most countries the target of these initiatives are secondary school and higher education students. A practical example is given by the Czech and the Italian cyber security competitions, which have the highest number of participants and have effectively involved the whole education system in the promotion of their events.

Another a possibility could be to lower the entry requirements to access the competition, as only 25% of competitions require "basic" computer science skills in their qualifying rounds. Most of the time, competitions require intermediate computer science or cyber security skills (30%) or a combination of higher-level skills in computing and math. Higher and specialised entry level requirements make it more difficult for people with no experience to even signup to these competitions and get a taste of what cyber security might entail. Therefore, lowering entry level requirements could help more students to enter the field and decide whether cyber security is something that is of interest to them.

In the same vein, but also to balance a sector which is heavily male dominated, more work could be done to increase the gender diversity of competitions. In fact, only between 5-10% of national competitions' participants are female. In this regard, a useful first start could be to look at the experience of the Czech-Republic, where, despite the absence of a specific policy to promote diversity, the national competition can boast a male to female ratio of approximately 70:30, which can be attributed to a strong public affair strategy and NGO involvement in competition's organization. In a context where increasing the number of participants should be among the goals for the majority of national competitions, a common ECSC Roadmap would have to solve an intrinsic issue: how can a national competition involve the largest and most diverse group of individual, at least initially, and later be able to select a small elite of gifted students to enter the ECSC?

NCSCs should have one long or multiple phases where participants are first taught new cyber security knowledge and skills and then are selected to attend the ECSC

A possible solution to this issue could be for a common ECSC Roadmap to encourage a greater standardization of the competition's organization, namely in the number and length of phases a competition should have. Section 3 proposed that national competitions should adopt a model with at least one qualifying round and a final, which indeed seems the case for most of the national competitions in the survey. However, there are still serious differences within this model, most notably in the length of the competition's phases, whether a formal training is incorporated before a national final and who it targets. As it is not hard to see how competitions that last for longer can be more beneficial to students in terms of increased learning opportunities, the authors of this report believe that national competitions should have one long or multiple qualifying rounds, where participants are ideally taught new cyber security knowledge and skills as they progress and before entering a final competition. The final challenge should then be concerned with selecting the best young talent to attend the ECSC. This model would help to involve a larger set of individuals in the first phase, and then progressively screen more candidates until a small team of elite student is found. The benefits of having longer national cyber security competitions is also supported by the hands-on experience of some national organizers. One interviewee stated that recently his organizations changed his format from the traditional 24-48h CTF format to a 2 week-event, which gave participants more time to study on their own and solve more challenges: "This is important with regards to our objectives stated above in cultivating the knowledge, skills and culture of individuals, albeit at the cost of narrowing down the selection for the final ECSC team." Similarly, another national expert revealed that his organization has recently changed the training format, from a two-weekend onsite bootcamp to a continuous online training and participation in international competitions, based on the realization that "in such a short time (two-weekend onsite bootcamp), it is very difficult to teach cybersecurity, especially to the youngest participants."

Finally, an important element of this model would be to make sure that participants who are "hooked" and at least initially involved in the competition are kept involved throughout the event.

It is understandable that a competition whose goal is to identify cyber security talent could be "impatient" to select its dream team and send it to compete in the ECSC. However, it is probably counterintuitive trying to encourage more and more young people to participate in a national competition and then not engaging them if they do not manage to pass the first round. If a student is interested in cyber security, but he/she is given no chances to nurture this interest, the labour market will unlikely see more cyber security professionals in the next future. In this regard, survey results show that only 25% of national competitions keep involving the participants who do not make it to the final round, while 25% keep involving them "somewhat." Similarly, national competitions seem to be struggling to keep their user "active" as only 17% of those who signup continue to be engaged. It is very important to keep involving the students who do not make it to the final round. There is emerging evidence of the fact that participants who do not make it to the final rounds could be at least as interested (if not more interested) in cyber security and its careers than their gifted pears who make it to the final.54 If this is true, and in the context of the lack of cyber security professionals, it would be a lost opportunity for a cyber security competition to disengage these students from the sector, especially given the efforts undertaken to "hook" them. There are multiple ways through which this can be achieved, for example by giving the participants the opportunity to engage in some of the same challenges that their peers are asked to solve in the final or through online learning. In this case, a practical example would be the Italian OpenCyberChallenge.IT program, which allows students who are not admitted to the training/final round to follow online lectures, get and solve challenges and receive a certificate of participation after completion of the program (see pg. 46 for further details).

5.5.2 Cyber security challenges, training and technological infrastructure

Section 3 underlined the importance of training as one of the core components of a national cyber security competition, which should incorporate both technical and soft skills in the curriculum. It also highlighted that there is no particular agreement among experts on the type, duration and length of training.

Survey results confirm that national cyber security competitions tend to have vastly different training methodologies, each of them with their pros and cons. At present, approaches are so diverse to make it hard to even have a simple comparison across countries. For example, survey results show that almost 1000 individuals are trained in cyber security skills across the EU and ECSC partner countries during cyber security competitions. However, approximately 70% of these participants are trained in only three countries. Moreover, the target of this training is also different. Whereas most countries train only those participants who later attend the ECSC, (very) few countries train a broader number of individuals, in addition to those going to the ECSC. Finally, survey results show that there are different approaches also when it comes to the length of training, with 80% of national cyber security competitions training participants for less than 3 months.

Considering this great variety of approaches, a common ECSC Roadmap should encourage national cyber security competitions to standardise cyber security training. The authors believe that establishing what the word "training" means in the context of a national cyber security competition and what its key features should be (duration, type, content and target group) are the number one priorities for a common ECSC Roadmap. As previously touched upon, the authors would argue that, in principle, national cyber security competitions should aim to train the largest number of participants for the longest period possible or an amount of time that participants and organizers find conducive to develop and consolidate a good level of cyber security knowledge and skills. In other words, the authors think that a national cyber security competition that trains over 100 students for more than 3 months have higher chances to achieve the objectives that a competition should meet (see section 5.1) rather than a

[54] https://gtr.ukri.org/projects?ref=studentship-1938110

competition that trains 10 individuals for 1 week. Moreover, the authors believe that a national competition should aim to train participants beyond the small group of individuals (typically 10) who are part of the national teams attending the ECSC. If it is true that cyber security competitions are established with the intent to reduce the shortage of cyber security professionals, national competitions should also aim to train people who are interested in a cyber security career, and not only the already gifted small minority who attends the ECSC. As previously mentioned, there is emerging evidence about the fact that students not making to the final round are likely to be as interested in cyber security as their peers who achieve the final challenge. Hence, envisaging some sort of training even for the "excluded" could indeed be beneficial to increase cyber security skills in students who might end up pursuing a cyber security career even if excluded from the ECSC team. As of now, very few national competitions also train those participants that do not attend the ECSC.

Moreover, the platforms used by different countries for the deployment of competition challenges and the training also differ vastly as indicated in table 3. Some of the platforms are free and open source with limited functionality like CTFd while other are commercial products with extended functionality like hacking-lab. In the presence of relevant budgets differences , one can notice some countries using expensive and state of the art commercial platforms for the training of their national teams, whilst other countries are struggling to even provide soft drinks during the competition. This does not provide a level playing field to participants overall. Thus, a common ECSC Roadmap should encourage the establishment of a central repository of cyber security challenges developed using standard formats and platforms to help different countries to have at their disposal updated cyber security challenges.

The first priority of an ECSC Roadmap would be to encourage a greater standardization of cyber security training in NCSCs

Finally, knowledge sharing can help countries that struggle to organize national competitions according to certain standards and, in doing so, elevating the quality of cyber security learning across the EU and ECSC partner countries. In the survey, 4 countries reported that they do not have the technical capabilities to organize such competitions and are struggling to identify relevant sources of information. On the other hand, 8 countries are willing to provide assistance. The referred technical capabilities are mainly related to the development and deployment of technical challenges. These challenges differ vastly from country to country and every country is following their own methodologies as indicated in section 4.5. This different approaches in challenge development impacts the overall quality of the competition, for example when a national cyber security competition does not take into account the difficulty levels for new commers, which might unintentionally demotivate them to participate in future challenges.[28,29] To solve this issue, a standardized challenge format and deployment platform could be developed thanks to the extensive expertise and knowledge sharing of participating countries. This will result in standard skills assessment and training to further improve the already well-defined ENISA curriculum and to increase the overall quality of the competition. Moreover, such multinational collaborative effort takes out the burden from individual countries competition organizers for setting up the whole competition technical environment on their own. This will save both time and money for the organizers, enabling them to address more organizational challenges like increasing diversity and promote cyber security awareness.

5.6 CONNECTION WITH EMPLOYERS AND CAREER OUTCOMES

Survey results confirmed that increasing interest in cyber security careers and connect participants with employers should be one of national cyber security competitions' objectives (section 5.1). Section 3 argued that, in order to achieve this objective, it is essential to establish and strengthen relations with employers, create a network of alumni and organizations to help participants understand more about cyber security careers and organize networking events/career fairs..

Survey results show that national cyber security competitions could do more to develop their links with employers and better liaise participants with the cyber security labour market. In fact, 20% of competitions try "somewhat" to link participants with employers, while another 20% do

not have such mechanisms in place; only half of competitions have an alumni or mentors network; only 20% collect data on participants' career outcomes, which makes the quantitative assessment of competition success with regards to their career outcomes more difficult.

A common ECSC Roadmap should support countries to improve their career and employability outcomes. There are several ways to achieve this. For example, competitions could collect participants' CV and allow employers to view them in a online custom platform; social and career fairs could be organized to make students more informed about cyber security roles and organizations; finally employers could be encouraged to offer placements and internships to competition's participants.

Besides these practical elements, a common ECSC Roadmap should perhaps promote a mind-shift among practitioners on the importance of competitions as a tool to increase the number of cyber security professionals in the labour market. Survey results show a sort of "under commitment" to cyber security careers, which also seems confirmed by the list of objectives in section 5.1, ranking "increase interest in a cyber security career and connect participants with employers" as only the 4th objective. As stated above, the authors believe there should be more emphasis on this objective. Competitions should put in place activities that effectively bring closer participants with employers, without assuming that simply organizing and running a competition will somehow automatically mitigate the lack of cyber security professionals. Instead, well thought-out activities that ensure a strong and systematic connection between participants and employers should be created to make participants aware of cyber security professional opportunities.

NCSCs should put more effort in linking participants with employers and encourage them to consider a cyber security career

5.7 ENISA'S ROLE

Finally, the survey asked national organizers what role should ENISA play to further support national cyber security competitions in the EU and affiliated countries. The most mentioned suggestions include:

- Propose/support dissemination, marketing and public affair activities;
- Provide and share cyber security challenges/training material;
- Increase the visibility of national competitions among governments;

Other interesting, albeit less mentioned, tasks are:

- Host the ECSC and provide funds to the national teams to attend the event;
- Help overcoming the gender issue;
- Providing best practices in running national competitions.

The authors believe that in the process of establishing a common ECSC Roadmap, ENISA can effectively increase its role and provide added value in the activities listed above. Some of them can be implemented rapidly and at relatively low cost. For example, ENISA could help national competitions gather the support of national public authorities by leveraging the Agency's network of national contact points and policymakers; national competitions' dissemination and public affair activities can be further coordinated with the Agency's activities in the same field. Moreover, and in line with its tradition of applied studies, ENISA could also conduct additional research on best practices in running national competitions and provide the necessary evidence basis for a common ECSC roadmap. Other tasks such as the provision of cyber security challenges/training material, assistance in overcoming the gender issue and hosting the ECSC probably require further elaboration, but are objectives worth discussing depending on the future of the ECSC as an EU policy.

6. CONCLUSIONS AND RECOMMENDATIONS

This report aimed to identify the key factors enabling the success of a national cyber security competition and to give a snapshot of the current situation in the EU and ECSC partner countries. To do that, we conducted a dozen interviews with national and EU experts, searched and reviewed the relevant scientific literature and collected data on these key enabling factors with a survey, which was filled by 90% of the countries attending the ECSC. This was done to provide preliminary insights and a discussion platform to determine a common ECSC roadmap, which is presented below.

At present, there are many similarities among national cyber security competitions and thisis a good starting point for the development of a common ECSC roadmap. However, there are also many differences on several key aspects, making the definition of a common ECSC roadmap an important and urgent task, if stakeholders wish to develop the ECSC at its fullest potential.

In light of this research, we believe that establishing and implementing a common ECSC roadmap with a view to promote a standardisation of national cyber security competitions has the potential to make the ECSC the EU flagship policy in the field of cyber security education. This would place the ECSC in a primary position to support the objectives of the EU Security Union Strategy for the period 2020-2025. We believe so because we currently do not see many other policies that, like the ECSC, could potentially involve 20.000 students, provide solid cyber security training to almost 1.000 individuals and give such visibility to EU efforts in cyber security policies.

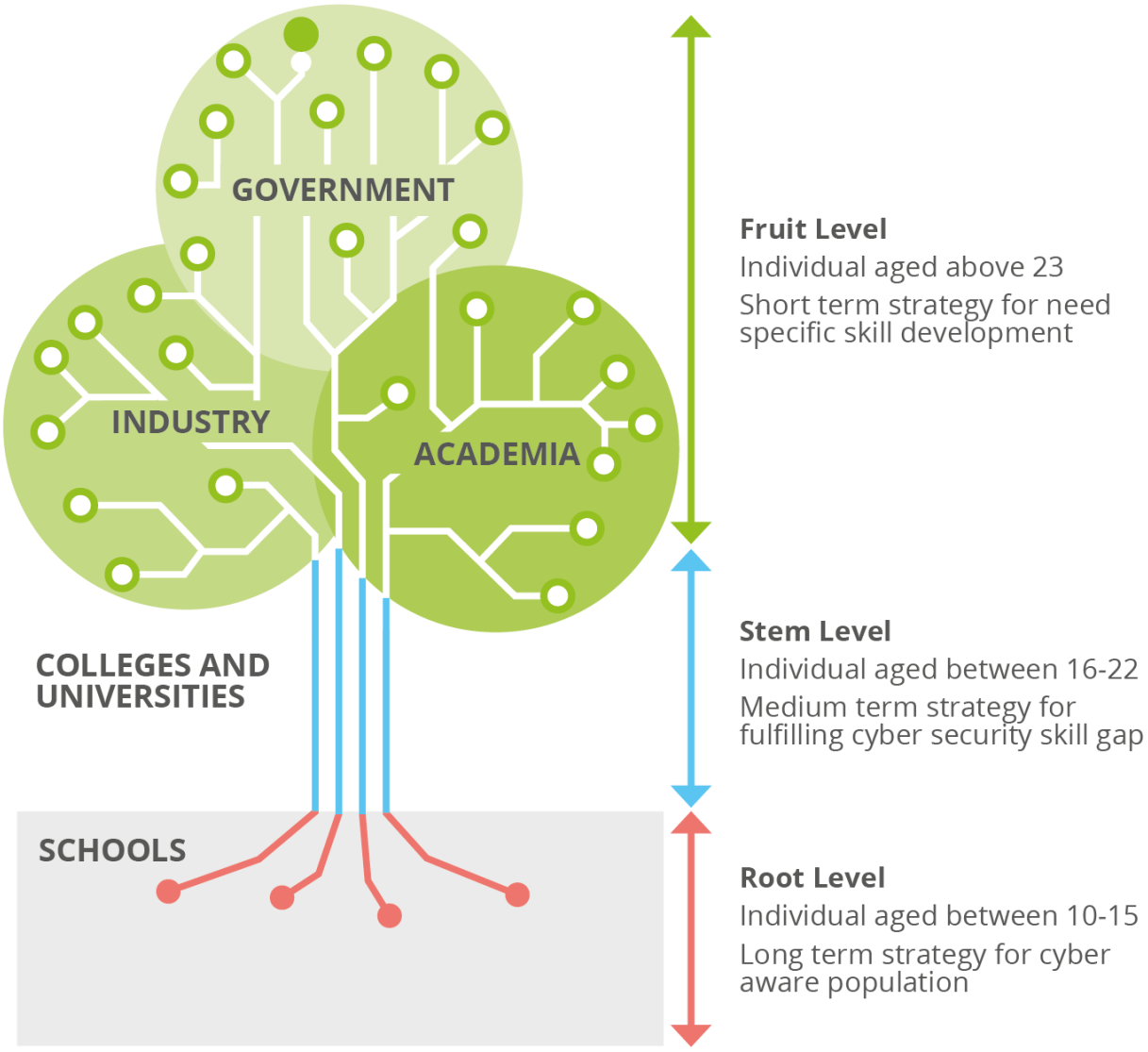
We use the analogy of a tree and its roots to summarize our findings (Figure 4). A tree has a strong foundation at the roots level, which provide the necessary strength for the stem to grow. When the stem becomes strong enough different, the branches of the tree start to spread out and bear fruit. To accomplish ECSC's objectives there also is the need for a strong foundation. This can be achieved by involving students and the public in a nationwide competition like in the Czech Republic, which saw the participation of more than 5000 individuals in the first round of the competition (Table 1). This also helped in increasing awareness at a national level which motivated a diverse group of individuals to participate in the competition without having a specific policy for promoting diversity.

When the root level is established, then the stem flourishes. The example of Italy can be taken, where they are using a systematic and institutional approach for identifying and training young cyber talent. Their universities and other educational organisation can take part to the national cyber security competition and provide training to a team of students who then attend a local and a national challenge (Section 4.6.2). This not only makes the competition more competitive, but also acts as tool for spreading cyber security knowledge among different geographical areas, which helps creating small clusters of cyber security hubs within each region. The positive results of this approach are underlined by the performance of team Italy in the ECSC 2017, 2018 and 2019 editions, when the Italian team ranked 3rd, 6th, and 2nd place, respectively. It should be noted that winning a competition is one thing and creating a systemic learning environment to address the cyber security need for the country is completely different, in that regard lessons from Czech Republic and Italy can be learned.

Now, when the stem flourishes the tree starts bearing fruits. At this stage different countries try to provide employability to the identified cyber talent. The effort of Spain in this regard are

admirable, as it follows a well-structured process to identify, attract, train, recruit, and place the next generation of cybersecurity professionals. Every year, they organize the Cybersecurity Employment and Talent Forum, which is designed to show students what it is like to work in the industry, provide them with the chance to meet industry experts, explore potential careers, discover education opportunities and learn about practical next steps (Section 4.7). Other countries like Czech Republic, Italy, Germany also organize similar events.

Figure 5: Common model for organizing NCSC



Therefore, in light of what suggested by national experts and the scientific literature (section 3), survey results (section 4) and the subsequent analysis (section 5), a common ECSC Roadmap should have the following objectives:

- Identify young cyber security talent
- Increase interest in cyber security as a topic
- Increase cyber security knowledge and skills
- Increase interest in a cyber security career and connect participants with employers
- Create a network of young cyber security specialist

A common ECSC should renew emphasis on the objective "Increase interest in a cyber security career and connect participants with employers" and related activities (see recommendations on "connection with employers and career outcomes" below) in the light of the current shortage of cyber security professionals and run rigorous evaluations to see whether these objectives are successfully achieved based on the indicators in section 3.1;

Based on the key enabling factors identified in section 3, a common ECSC Roadmap should:

6.1 POLICY RELEVANCE, GOVERNANCE AND PPP

- Encourage more countries to understand the strategic importance of their national cyber security competitions in the field of cyber security education, in the context of the cyber security skills shortage;
- Encourage countries to make national cyber security competitions more "policy relevant," for example by mentioning them in their national cyber security strategies, and to adopt a more systematic policy and vision on cyber security education;
- Noting that perfect governance structure for a national cyber security competition does not exist, encouraging the establishment of a PPP involving the key actors of the national cyber security ecosystem is likely to provide several benefits;
- Encourage those countries where a national competition is organized and implemented by only one actor to involve more stakeholders and reap the benefits of a public-private partnership, when this is feasible and practical;
- Encourage governments to more firmly support and assist national cyber security competitions, especially when they are in their "start-up phase" and when the rest of the national cyber security ecosystem cannot adequately back them.

6.2 FUNDING

- Make sure national competitions have appropriate financial resources to meet their current objectives;
- While a perfect funding arrangement does not exist, supporting a model in which costs are shared among key actors, most notably the government and the private sector, could provide more financial stability over time;
- Encourage the 35% of countries who receive funding from a single source to attempt to diversify the sources of their budget, when this is feasible and practical;
- Consider whether governments and the EU should increase their financial support to assist in the development of the ECSC as a fully-fledged EU cyber security policy and ensure a level playing field for national cyber security competitions. Without adequate financial support, in the current state of affairs, it would be impossible, and possibly unfair, to ask national cyber security competitions to initiate any Common ECSC Roadmap process;
- Take note of ENISA 2017 recommendations [48] and adopt the following funding strategies:
    - Offer attractive sponsorship to the private sector to enhance their marketing presence for example in national level events;

- Organize side events like conference, trainings and job fairs and have entry-fees ;
- To overcome geographic disparities and avoid unnecessary carbon emissions from traveling, use video-game streaming technologies to their full potential.

6.3 PUBLIC RELATIONS AND MARKETING STRATEGY

- Encourage 40% of national cyber security competitions without a fully developed public relations, marketing and communication strategy to establish one;
- Develop a public relations and marketing strategy taking into account the following objectives:
  - Promote the event and raise cyber security awareness (see below);
  - Reach out to potential participants and increase recruitment (see below);
  - Give visibility to sponsors and the national cyber security ecosystem;
  - Build a positive narrative around cyber security and inform stakeholders about the competition's success stories.
- Coordinate national competitions public affairs activities with ENISA;
- Establish a repository of communication best practices to assist countries in developing their own communication and marketing plan.

We believe a common road map should have three phases at national level to increase cyber security awareness, which will result in increased participation of a diverse group (Figure 4):

1. A phase to spark interest in young people 10-15 years old with the following features:
   - Preferably in cooperation with primary schools as part of the curricula;
   - This should be fun and based on gamification, with a hint of competition;
   - Focus on broad interest and education.
2. An inclusive national CTF phase for 16-22 years old with the following features:
   - Based on local CTF clubs;
   - Preferably in cooperation with a national e-sport organization and universities;
   - Focus on continuous learning and skill improvement.
3. Main phase nationally and internationally for 16-25 years old with the following features:
   - Preferably made media friendly in order to have more media exposure in mass media;
   - This also creates attractive venues for sponsor visibility;
   - Focus on the elite and winners.

Furthermore, we recommend defining policies to make cyber security relevant for a broader audience. This can be achieved by involving the education sector and national ministries of education in the dissemination of information related to the national cyber security competition during the recruitment phase and by establishing close coordination between high schools, universities, public and private sector to organize through:

- Research days at universities and invite general public to showcase latest cyber security technologies;
- Career days at public and private organizations for high schools and university students to spark interest in cyber security careers;
- ECSC alumni meetups for sharing knowledge, experience and opportunities among each other.

Finally, we recommend engaging:

- Schools and universities by placing attractive competition banners in prominent places like libraries;

- Social media platforms that are mostly used by young people, using photo and video sharing applications.
- The audience during such competition events, with live commentary and explanation of technical things.

6.4 TRAINING AND THE COMPETITION

- Set guidelines on how to assist countries to attract a higher number of participants in the first qualifying round of the competition, paying close attention to the examples offered by the Czech and Italian approaches.
- Reflect whether having lower entry level requirements (basic computer science skills versus intermediate/advanced computer science and cyber security skills) could help to attract a higher number of participants in the initial qualifying round, when this does not impact the overall quality and development of the competition;
- Increase the gender diversity of competitions by paying close attention to the Czech example, which is currently the only national competition with a 70:30 male to female ratio;
- Set guidelines and standards on how to ensure that most students who signup remain active throughout the competition, considering the examples offered by the Austrian, Italian and Romanian competitions;
- Encourage a greater standardization of the competition's rounds and/or phases: the authors of this report believe that national competitions should have one long or multiple qualifying rounds, where participants are given the chance to learn new cyber security knowledge and skills before entering the final challenge selecting the ECSC national team;
- Encourage national cyber security competitions to standardize cyber security training, including:
  - Define the concept and meaning of "training" in the context of a national competition;
  - Define and establish the key features of training in terms of duration, type, content and target group. As an overarching principle, a national cyber security competition should aim to train the largest number of participants (beyond those attending the ECSC) for an amount of time that is appropriate to consolidate a good level of cyber security knowledge and skills;

Moreover, we recommend the establishment of a joint working group comprising of members of different participating countries with the following responsibilities:

1. Define cyber security challenges' standards and their deployment platform;
2. Provide assistance to countries that have technical challenges in implementing such competitions;
3. Create a central repository of challenges where countries can donate and use different challenges if needed;
4. Coordinate with different government, academic and private stakeholders to keep cyber security challenges relevant as per their interests.

The establishment of the working group will ease the burden on national organisers. This will enable them to focus more on organizational aspects of the competition such as for example funding and public affairs. Recommendations on these aspects were already proposed by ENISA. One key point for challenge development is their adaptability to be used in different organizational setting. As the basic objective of the ECSC is to identify young talent and increase cyber security awareness, the challenges are helping to identify young cyber talent. However, to increase cyber security awareness these challenges should be able to be used other than the competition environment. This will help sharing the challenges among different government, academic and private stakeholders for their internal training and security awareness as well. This can be achieved through defining a standard for security challenge development and deployment.

6.5 CONNECTION WITH EMPLOYERS AND CAREER OUTCOMES

- Promote a mind-shift regarding the importance of competitions as a tool to increase the number of cyber security professionals in the labour market;
- Support national cyber security competitions to improve their career and employability outcomes and encourage them to organize activities that effectively and systematically bring closer participants with employers, such as:
    - collection and dissemination of participants' CVs;
    - career and networking events;
    - employers-led lectures;
    - establishment of alumni networks;
    - guaranteed placements opportunities such as internships and traineeships.
- Monitor the career progression of competitions' participants by:
    - Collecting information of online professional profiles of participants;
    - Conducting anonymized surveys on former competition's participants about their carrier progression;
    - Conducting personalized interviews with participants related to their carrier progression.

6.6 ENISA'S ROLE

- Should consider as a matter of priority to increase its role in the following activities:
    - Increase the visibility of national competitions among governments;
    - Coordinate national competition's dissemination activities;
    - Conduct additional research on best practices in running national competitions and provide the necessary evidence base for a common ECSC roadmap;
- Other activities it should consider:
    - Provide and share cyber security challenges/training material;
    - Give guidance on how to ensure that a pool of people with a broader education and gender variety is involved in national competitions.

TP-01-21-016-EN-N

ABOUT ENISA

The mission of the European Union Agency for Cybersecurity (ENISA) is to achieve a high common level of cybersecurity across the Union, by actively supporting Member States, Union institutions, bodies, offices and agencies in improving cybersecurity. We contribute to policy development and implementation, support capacity building and preparedness, facilitate operational cooperation at Union level, enhance the trustworthiness of ICT products, services and processes by rolling out cybersecurity certification schemes, enable knowledge sharing, research, innovation and awareness building, whilst developing cross-border communities. Our goal is to strengthen trust in the connected economy, boost resilience of the Union's infrastructure and services and keep our society cyber secure. More information about ENISA and its work can be found at www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Greece

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

enisa.europa.eu

ISBN 978-92-9204-464-0
DOI: 10.2824/657311