EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ECSC 2020 ANALYSIS REPORT

Maturity assessment of and lessons learned from the European Cyber Security Challenge 2020

APRIL 2021

About ENISA

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

Contact

To contact the authors, please use ecsc@enisa.europa.eu.
For media enquiries about this paper, please use press@enisa.europa.eu.

Authors

Adrián Belmonte Martin and Ioannis Agrafiotis – European Union Agency for Cybersecurity; contributions from the report on lessons learned and the public affairs strategy by Arttic and Weber Shandwick.

Acknowledgements

We would like to thank all our colleagues responsible for the national competitions and the preparation of the teams that participate in the European Cyber Security Competition. Without their untiring efforts, this competition would not be possible.

Legal notice

Copyright notice

ISBN: 978-92-9204-496-1 - DOI: 10.2824/284260

EXECUTIVE SUMMARY

The 7th edition of the European Cyber Security Challenge (ECSC), planned initially for 4 and 5 November 2020 in Vienna, had to be postponed because of the coronavirus disease 2019 pandemic. Considering that the organisation of this European event brings together more than 350 young people coming from all over Europe, the ECSC Steering Committee wants above all to safeguard the health of all participants.

Consequently, the committee, together with the Austrian national planners, with the support of the European Union Agency for Cybersecurity (ENISA) and the agreement of the future ECSC organising countries, decided to change the dates of the ECSC 2020 final and postpone the 7th edition to 2021.

Therefore, the 7th edition of the ECSC will take place in Prague, Czechia, in 2021. Austria will host the event in 2022.

Despite this, to maintain support for the growth of the competition, keep the spirit of the ECSC alive and prepare for the 2021 edition, various activities were performed during 2020, such as the first ENISA Hackfest, the initial steps towards the selection of Team Europe for the International Cyber Security Challenge (ICSC) planned for Athens in December 2021 and the launch of the ICSC Steering Committee, responsible for the international competition.

ENISA is currently hosting a number of platforms and performing several activities to support the ECSC hosting country and the future development of the project, including hosting the ECSC main website, hosting the ECSC planning platform, working on the public affairs strategy, creating challenges, overseeing the governance framework of the competition and providing support for the ECSC Steering Committee as the acting secretariat.

In order to ensure appropriate and transparent reporting to the ECSC Steering Committee, the following key observations were made by independent third-party observers who attended ECSC 2020 planning meetings. These observations were made based on the feedback collected from participants, members of the ECSC Steering Committee and attendees at the Hackfest event, including through an online evaluation survey and personal interviews.

- Concerning the way in which the 2020 cancellation was managed, it was stressed that the transparency shown by ENISA and its involvement of the ECSC Steering Committee in the decision-making were good. Decisions were made in agreement with all countries concerned, for example on how to communicate the cancellation of ECSC 2020.
- There is no need for the committee to do things very differently. Some improvements could be made to accelerate the circulation of official documents when finalised and to clearly state who is to receive ECSC-related documents. Based on the responses to the organisers' questionnaire, 77 % of respondents considered that the ECSC Steering Committee performs well.
- A clearer dissemination plan would be helpful, but there is also a need to establish a transmission channel between the ECSC public affairs team and contractor on the one side and national teams on the other. Many ECSC participants would welcome messages and communication materials crafted at ECSC level. This should include infographics and other visual elements to help to ensure that posts on Twitter or on participants' websites are eye-catching and engaging.

- Regarding ENISA Hackfest 2020, based on the questionnaire sent to participants, 76 % of respondents considered that the performance of the platform was good or excellent. No major issues or incidents with regard to the availability of network infrastructure were reported by respondents to the questionnaire or in interviews.

In addition, it seems worth noting that some of the open-ended comments made by the ECSC Steering Committee members who participated in the study concerned:

- the strengthening of the European dimension of the ECSC;
- the need to preserve the ECSC's spirit of fun;
- the balance to be struck between opening the competition to as many countries as possible and logistical and financial issues;
- the need to develop a sense of a community and to build a community inclusive of women and very young participants;
- the need for reflection on ways to attract more women into the cybersecurity field;
- the possibility of tapping into the pool of expertise formed by ECSC members.

The final of the 2021 edition of the ECSC will take place in Prague in September 2021; at least 22 countries are expected to participate. The latest updates will be published on the ECSC 2021 website (https://www.europeancybersecuritychallenge.eu/).

This report is not for public dissemination. It concerns only ENISA and the members of the ECSC Steering Committee, namely the representatives of the countries that participate in the ECSC.

TABLE OF CONTENTS

ABBREVIATIONS

API	application programming interface
CET	Central European Time
COVID-19	coronavirus disease 2019
CIRCABC	Communication and Information Resource Centre for Administrations, Businesses and Citizens
CTF	capture the flag
ECSC	European Cyber Security Challenge
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
FAQ	frequently asked question
ICSC	International Cyber Security Challenge
KPI	key performance indicator

1. INTRODUCTION

The growing need for IT security professionals is widely acknowledged. According to recent estimates, it is expected that more than 3.5 million cybersecurity professionals will be needed worldwide by 2021 ([1]) to prevent, react to and protect citizens from cyber threats. Europe has to make an effort to attract talent to and retain it in cybersecurity and, at the same time, create solid and powerful educational, entrepreneurial and business structures in cybersecurity.

To help mitigate this shortage of skills, many countries have launched national cybersecurity competitions targeting students, university graduates and even non-IT professionals, with a clear aim:

'Identify new and young cyber talents and encourage young people to pursue a career in cyber security.'[2]

The European Cyber Security Challenge (ECSC) (https://www.europeancybersecuritychallenge.eu/) leverages on these competitions by adding a pan-European layer. Top cybersecurity talents from each participating country meet to network and collaborate and, finally, compete against each other. Contestants are challenged to solve security-related tasks in different domains.

In a nutshell, ECSC is the annual European event that brings together young talent from across Europe to have fun and compete in cybersecurity. Its main aim is to highlight the importance of the national competitions.

In a nutshell, ECSC is the annual European event that brings together young talent from across Europe to have fun and compete in cybersecurity. Its main aim is to highlight the importance of the national competitions.

1.1. Background to the ECSC

The project was initiated under the umbrella of the European Union's cybersecurity strategy of February 2013, which stated that the European Commission would:

'organise, with the support of ENISA, a cybersecurity championship in 2014, where university students will compete in proposing [network and information security] solutions.'[3]

Since 2014, the European Union Agency for Cybersecurity (ENISA) has been supporting the organisation of the ECSC. ENISA actively organises the meetings of the governance structures, supports the development of the competition's rules and challenges and is part of the ECSC jury. Since 2016, ENISA has been the acting secretariat of the ESCS Steering Committee.

In the 2018 edition, 200 participants (contestants, coaches and judges), representing 17 EU and European Free Trade Association (EFTA) countries (Austria, Belgium, Cyprus, Czechia, Denmark, Estonia, France, Germany, Greece, Italy, Liechtenstein, Norway, Poland, Romania, Spain, Switzerland and the United Kingdom), competed in the ECSC final in London.

The 2019 edition of the ECSC took place in the parliament building in Bucharest, Romania, from 9 to11 October 2019. For the first time, teams from 20 countries participated in the final (Austria, Cyprus, Czechia, Denmark, Estonia, France, Germany, Greece, Italy, Ireland, Liechtenstein, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland and the United Kingdom).The participants investigated vulnerabilities in web applications, binaries and

([1]) https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis
([2]) ECSC Charter document
([3]) https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667

document files; solved crypto puzzles; and hack hardware systems. However, technical skills are just one part of the story. Time and resources were limited, and teamwork and presentation skills were also evaluated. The top teams in ECSC 2019 were the teams from Romania, Italy and Austria.

The 2020 edition of the ECSC, planned initially for 4 and 5 November in Vienna, had to be cancelled owing to the coronavirus disease 2019 (COVID-19) pandemic.

The 2021 edition of the ECSC will take place in Prague, Czechia, on 29 and 30 September.

1.2. The ECSC set-up

Each country is represented at the ECSC final by a team of 10 contestants, comprising the winners of the national competition. Half of them are 14–20 years old and half are 21–25 years old.

Two preparatory pilot phases of the ECSC were held in 2014 (in Austria) and 2015 (in Switzerland), attended by three and six countries, respectively. Since 2015, ENISA has used its experience and position to coordinate and organise the ECSC and enable it to reach full maturity.

The activities of the ECSC are supervised by a steering committee, composed of representatives of the attending countries. ENISA facilitates the meetings of this group and provides strategic guidance. The decision-making processes are described in the ECSC Charter, which is revised and approved every year by the ECSC Steering Committee.

ENISA is currently hosting a number of platforms and performing several activities to support the ECSC hosting country and the future development of the project, including hosting the ECSC main website, hosting the ECSC information-sharing platform, working on the public affairs strategy and creating challenges.

In addition, ENISA is working closely with the hosts of future editions in order to ensure appropriate and transparent reporting to the ECSC Steering Committee.

Each year, two ECSC Steering Committee meetings are held prior to the event:

- the initial planning conference in February or March,
- the main planning conference in June or July.

ENISA organised these preparatory events and had overall responsibility for the efficient running of the project, including minuting meetings and following up on proposed actions.

2. TRENDS IN ECSC ATTENDANCE

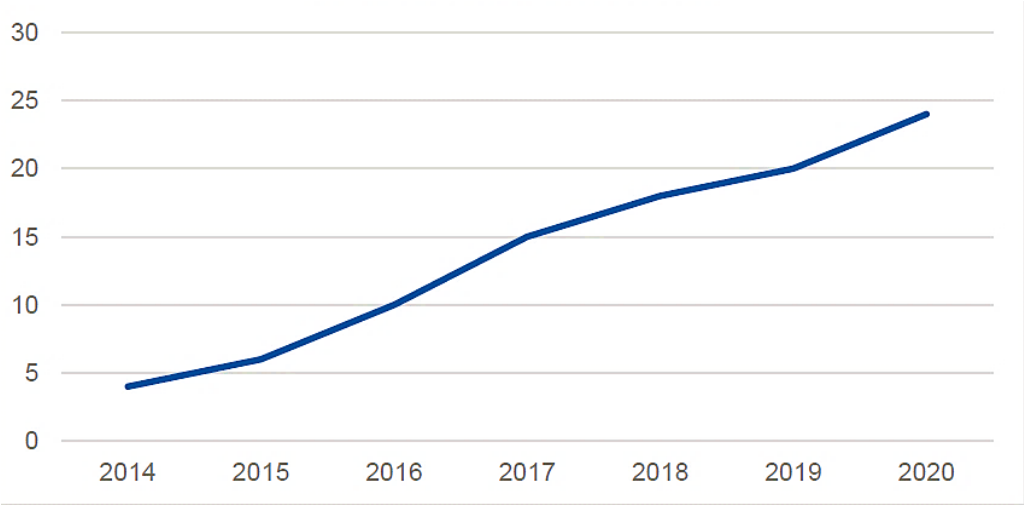
2.1. ECSC attendance

Since the first edition of the ECSC in 2014, the countries that have attended are the following.

- **2014 (3).** Austria, Germany and Switzerland.
- **2015 (6).** Austria, Germany, Switzerland, Spain, Romania and the United Kingdom.
- **2016 (10).** Austria, Estonia, Germany, Greece, Ireland, Liechtenstein, Romania, Spain, Switzerland and the United Kingdom.
- **2017 (15).** Austria, Cyprus, Czechia, Denmark, Estonia, Germany, Greece, Ireland, Italy, Liechtenstein, Norway, Romania, Spain, Switzerland and the United Kingdom.
- **2018 (17).** Austria, Belgium, Cyprus, Czechia, Denmark, Estonia, France, Germany, Greece, Italy, Liechtenstein, Norway, Poland, Romania, Spain, Switzerland and the United Kingdom.
  2019 (20). Austria, Cyprus, Czechia, Denmark, Estonia, France, Germany, Greece, Italy, Ireland, Liechtenstein, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland and the United Kingdom.
- **2020.** Owing to the COVID-19 pandemic, the competition was cancelled, with the 2022 edition to be held in Vienna instead.

Figure 1 depicts the growth of the ECSC since ENISA became involved in the competition in 2014.

Figure 1: Number of countries participating in the ECSC, 2014–2020



2.2. Participation in the ECSC Steering Committee

In the past 12 months, the following new EU and EFTA countries have joined the committee:

- Croatia
- Iceland
- Latvia
- Slovakia
- Slovenia.

The full list of members participating in the ECSC Steering Committee is as follows:

- Austria
- Belgium
- Cyprus
- Croatia
- Czechia
- Denmark
- Estonia
- France
- Germany
- Greece
- Iceland
- Italy
- Ireland
- Latvia
- Liechtenstein
- Luxembourg
- Malta
- the Netherlands
- Norway
- Poland
- Portugal
- Romania
- Spain
- Slovakia
- Slovenia
- Switzerland
- the United Kingdom.

Total: 27 countries

3. ENISA'S CONTRIBUTION TO ECSC 2020

3.1. Steering Committee management

The activities of the ECSC are supervised by a steering committee composed of representatives of the attending countries. ENISA facilitates the meetings of this group and provides strategic guidance. The decision-making processes are described in the ECSC Charter, which is revised and approved every year by the ECSC Steering Committee.

During the preparations for ECSC 2020, ENISA was responsible for the following activities related to the management of the ECSC Steering Committee:

- platform maintenance and updates,
- mailing list management,
- updating and creating ECSC Steering Committee-related documentation,
- supporting the organisation of the initial planning conference in Vienna,
- organising follow-up meetings with the ECSC Steering Committee,
- organising a follow-up meeting with the ECSC 2020 chair,
- COVID-19 situational assessment,
- accommodation, execution and follow-up of ECSC Steering Committee requests,
- implementation of changes and suggestions collected through surveys and other feedback from previous editions,
- management of the public affairs support contract,
- management of the ECSC support contract,
- updating the public affairs strategy,
- creating various subcommittees and working groups to support new activities,
- deciding on the methods for the creation of Team Europe for the International Cyber Security Challenge (ICSC),
- organisation of a hot-wash meeting,
- collecting feedback through a report on lessons learned and a survey of participants.

3.2. Initial planning conference

On 13 and 14 February 2020, the ECSC initial planning conference was held in Vienna. The following topics were discussed during the meeting:

- the ECSC 2019 experience,
- presentation from Austria on plans for the 2020 edition (logistics, hotels, etc.),
- lessons learned from ECSC 2019,
- ECSC 2020 planning status,
- Brexit and new countries,
- update on the ECSC Connecting Europe Facility call,
- update on the ICSC,
- presentation of new platforms.

The following actions and decisions were agreed in the meeting:

- a code of conduct was to be created;
- credentials and vouchers were to be provided to enable access to the Austrian platform that was to be used during the competition;
- the presentations were to be eliminated in the next edition of the ECSC, with a subcommittee to be formed to submit proposals on the development of soft skills;
- a calculation tool was to be provided for checking the ages of the participants;
- two subcommittees were to be formed, with the following members:
    - Subcommittee No 1 on ICSC decisions:
        - Austria
        - Cyprus
        - Czechia
        - Germany
        - Ireland
        - Luxembourg
        - Portugal
        - Spain
        - ENISA.
    - Subcommittee No 2 on soft skills:
        - Austria
        - Czechia
        - France
        - Germany
        - Greece
        - Norway
        - the Netherlands.

After the event, the minutes of the meeting were circulated to the ECSC Steering Committee for review and approval.

3.3. COVID-19 impact assessment

During the months of April and May 2020, ENISA and the ECSC Steering Committee chair/organising country (Austria) were continuously assessing the situation in order to monitor the impact of the COVID-19 pandemic on the participant countries and have available the information required to enable the best decision to be taken on holding the final in Vienna.

During May 2020, ENISA led the collection of information from the participant countries regarding the following issues:

- impact of the situation on national competitions,
- impact on meetings of national teams,
- measures taken and special considerations required,
- if the situation threatened national teams' participation in the final.

Given the *force majeure* of the situation and the measures imposed by the Austrian government, finally Austria decided that the competition needed to be either postponed or cancelled, and an ad hoc meeting between ECSC organising countries was arranged in order to present and consult on the different options. After the situation was explained, Norway, the 2022 host, and the subsequent organising countries agreed to the postponement of their competitions for 1 year and yielded the 2022 edition to Austria. It was not possible to postpone until next year because Czechia already had organisational commitments in place.

Following this agreement between Norway, Italy and Poland, the ECSC final will take place in Austria in 2022, Norway in 2023, Italy in 2024 and Poland in 2025. The 2021 edition remains the same.

After this agreement, on 18 May, an extraordinary ECSC Steering Committee teleconference was arranged to announce the postponement and the new dates for the competitions and to formally approve the decision.

In addition, at this meeting special measures to mitigate the impact of the situation were adopted by the ECSC Steering Committee, such as raising by 1 year the maximum age for participation in the 2021 competition.

Regarding the official announcement of the changes, the ECSC Steering Committee proposed that the participating countries create a joint communication plan, define a common message and coordinate media activities. A dedicated teleconference was organised by ENISA's public affairs team on 29 May. The official postponement announcement was launched on 3 June on the ENISA website (https://www.enisa.europa.eu/news/enisa-news/european-cyber-security-challenge-2020-dates-changed), followed by various social media activities. In addition, the ECSC official website was modified accordingly.

Figure 2: News item on the ENISA website announcing the postponement of ECSC 2020

3.4. International Cyber Security Challenge

Building on the success of the ECSC, ENISA, with the help of other regional and international organisations, decided to design and host the ICSC. The aim of the challenge is to attract young talent and raise awareness in the global community of the education and skills needed in the area of cybersecurity.

To this end, a steering committee comprising representatives of government and regional institutions and universities and research centres will design a competition between teams from different regions. So far, teams from South-East Asia, Oceania, the United States, Latin America and Africa have expressed a clear interest in participating.

Teams will compete in a series of challenges (to be decided by the ICSC Steering Committee) in a number of areas, such as web application and system exploitation, cryptography, reverse engineering, hardware challenges, forensics and escape rooms. The ICSC brand is expected to be associated with the top cybersecurity talents of the world, and ENISA anticipates that the ICSC will become one of the world's key incubators of cybersecurity entrepreneurship and top security experts.

ENISA is committed to organising the first ICSC final in Greece and supporting the development of the competition's rules and governing body. Each region will be represented at the competition by a team comprising young talent from countries in the region. The regions will be responsible for selecting and training team members. **ENISA proposes that the first ICSC final be held during the second week of December 2021. The international competition will be held in Athens.**

This competition can have a significant impact on strengthening cybersecurity; some of the objectives are the following:

- create and nurture a global multistakeholder cybersecurity challenge;
- strengthen international cooperation on cybersecurity;
- contribute to the world's strategy on cyberspace;
- promote capture the flag (CTF) competitions by leveraging to an international level;
- engage a wider audience and increase the level of awareness of the importance of holding events such as the ECSC;
- promote young talent across the world;
- promote cybersecurity training at an international level;
- develop various skills, including both technical skills and soft skills such as teamwork, presentation skills and public speaking;
- promote professional careers in cybersecurity by putting the young professionals in the spotlight and highlighting the interesting career paths available, in order to address the shortage of cybersecurity professionals.

During early 2020, ENISA completed the creation of the ICSC Steering Committee to support management activities. The committee:

- is composed of representatives of the regions that have committed to competing in the ICSC;
- is the ultimate decision-making body on the ICSC;
- defines the role and composition of the ICSC secretariat.
- provides leadership and direction on the scope and management of the work to be undertaken on matters that relate to the ICSC's scope and objectives, and related risks and issues, as necessary;
- acts in the best interests of the ICSC;
- provides steering and guidance on ICSC activities, while respecting the overall responsibilities of all stakeholders;
- is a delegated decision-making authority on the related activities within the scope of the ICSC;
- keeps relevant stakeholders informed on the ICSC and related developments.
- approves the ICSC Charter and the ICSC competition rules, accepts submissions from potential future hosting countries, decides on the dates and location of ICSC events, and makes decisions on any other issues arising, for example in the event of disputes.

Representatives of the various regions were engaged by ENISA during 2020 and began discussions to establish the required structures and the basis for the long-term development of future editions, namely:

- a consistent set of rules for the competition (ages and number of participants, requirements, etc.);
- the final curricula for the competition;
- the final format of the competition and the methods for maintaining a high level of transparency and trust between the regions.

ENISA, in the role of ICSC secretariat and organising body, executed the following actions in order to support ICSC activities:

- making initial contact with and engaging the International Steering Committee,
- creating a mailing list,
- creating a common roadmap,
- creating of space in the collaboration platform (Communication and Information Resource Centre for Administrations, Businesses and Citizens (CIRCAB)),
- organising follow-up meetings during the year,
- starting preparatory activities for the competition,
- developing key documentation,
- organising surveys and collection of information to support the decision-making process,
- carrying out activities to prepare for the final in December 2021.

3.5. ENISA HACKFEST 2020

On 16–18 November, ENISA hosted ENISA Hackfest 2020 (https://enisa-hackfest2020.cyberedu.ro/), a CTF event for cybersecurity professionals and students to connect and train the teams participating in the 2021 ECSC. Contestants were challenged on an individual level to solve cybersecurity problems in areas such as web security, mobile security, cryptography, reverse engineering and forensics. The Hackfest brought together more than 250 participants from 17 EU and EFTA countries. The event was held in a virtual format.

The event was to be used:

- as a testbed for future Team Europe selection activities;
- by ECSC national teams to assess future players' performance;
- as training for ECSC participants;
- to provide support to countries that cannot afford a national qualifying competition.

The event was hosted on a cloud-based platform (cyberEDU.ro) that can host large CTF competitions of various types, such as jeopardy, attack-and-defence and king-of-the-hill competitions, as well as competitions in other, more complex, formats such as cyber-range, classroom style, etc. The platform supports individual and team-based competitions. The technology can host events with as few as 10 players or as many as 5 000 and even more.

Figure 3: The ENISA Hackfest 2020 logo

3.5.1. Competition format

- Individual competition.
- Classroom style (teacher is visible only to his or her students).
- Jeopardy competition.
- All players registered to gain access to the challenges.
- Registration was available at the Hackfest website (http://enisa-hackfest2020.cyberedu.ro).
- Started on 16 November 2020 at 10:00 Central European Time (CET).
- Ended on 18 November 2020 at 10:00 CET.
- Team leaders received detailed reports after the event about each player, which included:
    - soft metadata such as nationality, age, sex, etc.;
    - technical statistics such as players' results, categories of challenges, timestamps, etc.

3.5.2. Train the trainers event

To provide information to the team captains and coaches, a train the trainers event was organised by ENISA and the contractor; this event was expected to provide clarification on various key issues:

- roles during the competition,
- rules,
- communication with and support from the organisers,
- challenges (types, difficulty, etc.),
- complaint management,
- scoring mechanisms,
- user management,
- reports and information,
- the look and feel of the platform,
- the registration process,
- flag submission.

In addition, access to a demo platform with real challenges was provided to participants before the event started, for testing purposes, and a trainer's manual was provided with all the relevant information.

The train the trainers event was organised virtually (using Cisco WebEx) on 6 November. A video and the manual were released on the ECSC collaboration platform and sent to the mailing list.

3.5.3. Hackfest results

- Total participants: 263.
- Total participants with positive score: 169.
- Total wrong attempts: 4 609.
- Total flags: 826.
- Gender statistics:
    - Men making attempts: 146.
    - Women making attempts: 3.
    - People who preferred not to say making attempts: 9.
- Average age of participants: 21.55 years.
- Number of countries participating: 17.
- Total challenges available: 24 challenges, 23 solved during the event, 21 solved by the best player.
- Fasted solve: 481 seconds, or 8 minutes and 1 second.
- Easiest challenge was solved by 128 players.
- Hardest challenge was solved by 2 players.
- On average, players solved 4.8876 challenges each during the event.
- Categories: Web security, Miscellaneous, Cryptography, Forensics, Steganography, Network security, Open-source intelligence, Mobile security, Memory analysis, Reverse engineering, Exploitation, Programming.

Table 1: Summary of challenges

Challenges			
Title	**Category**	**Total solvers**	**Final score**
hello-nemo	Miscellaneous, Forensics	128	50
downloader-v1	Web security	123	50
warmup-cat	Miscellaneous	99	50
fair-dice	Miscellaneous, Programming	71	50
imgur	Web security	49	50
what-to-do	Forensics	46	50
online-album	Web security	41	100
treasure-map	Miscellaneous, Open-source intelligence	40	110
s3-simple-secure-system	Reverse engineering, Cryptography	39	120
lukas-skywalker-business	Forensics	32	190
crypto	Miscellaneous, Cryptography	31	200
api	Web security	24	270
stargate	Miscellaneous	21	300
posts	Web security, Cross-site scripting	20	310
crow	Web security	16	350
investigator	Forensics, Miscellaneous, Mobile security	14	370
cerbebros	Web security	6	450
crack-me	Reverse engineering	6	450
spi-capture	Miscellaneous	5	460
ancient signal	Network security, Forensics, Cryptography	5	460
slot	Pwn	4	470
middleman	Reverse engineering	4	470
blindfold	Cryptography	2	490

3.5.4. ENISA Hackfest 2020 – lessons learned

3.5.4.1. Scoring

Dynamic scoring continues to be one of the most objective and accurate ways to evaluate the difficulty of challenges based on the technical level of players. The proposed algorithm worked as expected and no malicious behaviour was detected.

The potential risks and disadvantages of dynamic scoring are that:

- providing the same challenges to a group of players with different experience could give different results;
- malicious players could register additional fake users and solve a particular challenge in order to decrease the total number of points, providing an unfair advantage to other players who solve other challenges.

Lesson learned. ENISA recommends considering the use of dynamic scoring for any type of jeopardy competition but also keeping in mind the potential risks.

3.5.5. Challenges

The Hackfest Consortium set 26 challenges with 2 backups (14 previously used and 12 new challenges) for the event. No significant disruption of infrastructure was detected during the competition, but certain Layer 7-oriented attacks (mostly denial of service) were addressed.

Players who had previously solved the reused challenges found this situation unattractive and their tendency was to search for write-ups or use their previous solutions, rather than trying to solve the challenge again. However, many players did prefer to try to solve the challenges again and actually learn from this experience.

Lesson learned. ENISA recommends not reusing challenges in future.

3.5.6. Communication

The consortium took an innovative approach to communication this year, using an official Discord group with several communication channels.

Access to each channel was granted by a custom-made bot developed by the consortium. The bot granted access to channels to players based on invitation links, in accordance with predefined user roles (player, country coordinator and organiser). Moreover, the bot monitored communication between players and removed any message that potentially contained a flag or part of it.

The benefits were:

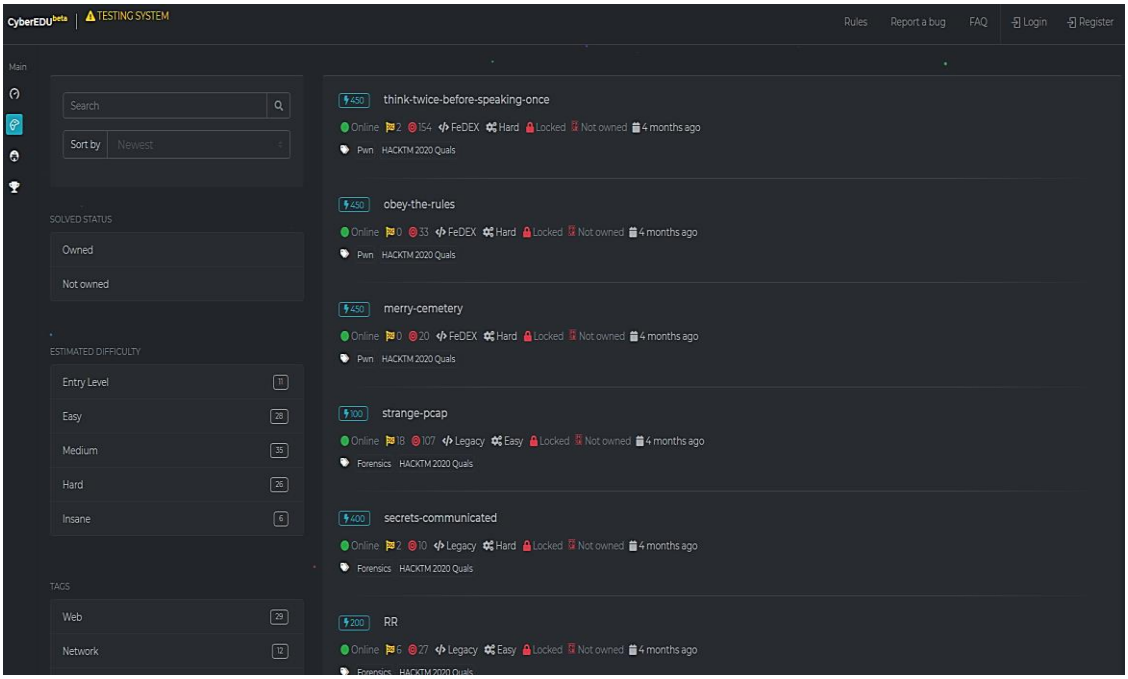
- voice chat, which allowed networking between players;
- flexible application programming interfaces (APIs), to enable the creation of bots with different levels of capabilities;
- very good and granular user access.

The disadvantages were that:

- the bot developer needed to introduce failover/healing features, since Discord APIs can have downtime quite often.
- voice chat could be used for flag sharing, bypassing the bot's control.

Lesson learned. Discord channels can be an alternative to Telegram or Slack for this type of event; however, certain issues must be taken into consideration.

Figure 4: The ENISA Hackfest 2020 platform



3.5.7. Support

In order to provide 24/7 technical support for 48 hours, the consortium used the following mechanisms.

- The challenge authors were available during the event and they answered questions when addressed.
- Each question answered was added to a common frequently asked questions (FAQs) document, which allowed the support team to answer common questions more quickly and focus on new or critical situations.
- During the night, at least one person was available at any point and was able to respond to all questions received.

Lesson learned. Developing a live FAQs document for challenges can speed up support resolutions during CTF competitions, which are quite intensive and exhausting for support teams if the event happens over several days.

Feature improvement. Another potential improvement would be adding a bot that can manage tickets, which could speed up the process, since a player would no longer have to wait for the identification of a staff member who was available to answer their question.

3.5.8. Complaints

Players and country coordinators had channels where they could make complaints. During the event, most of the conversations were challenge-related. The only question that could be construed as a complaint was related to the availability of rankings for individual players, so that participants could see how their country was situated in comparison with other countries.

3.5.9. Infrastructure and platform

The event was hosted on a cloud-based platform (cyberEDU.ro) that can host large CTF competitions in various formats. The platform and infrastructure had 100 % uptime during the event, with some minor issues during the first hour relating to reporting of results to country coordinators and organisers, which were immediately addressed by the consortium.

The benefits of using the platform, rather than other open-source/standard technologies, are as follows.

- **Management of the competition.** The platform allowed the consortium to set up and manage the event in minutes, with various custom fields at registration, multiple-level access (i.e.. organiser, teacher/country coordinator and player levels), dynamic scoring and more.
- **Scalability.** Since the entire application uses Kubernetes, the infrastructure can be scaled as needed for the existing load with no downtime recorded.
- **Moderation.** Having moderation support for registration allowed country leaders to accept or reject players.
- **Self-healing challenges.** The platform allowed players to vote for restart when a challenge seemed to be down or malfunctioning, and it automatically restarted the challenge when the system detected suspicious delays in response.

Lessons learned are the following.

- **Self-healing challenges.** These proved to be an improvement in terms of reducing staff effort required to manage the infrastructure; staff were able to solve downtime and malfunctioning from their phones.
- **One-to-one resources for players.** To further improve the experience of players, the platform used for future editions of the event should allow each player to run and restart their own instance of each challenge.

3.5.10. Miscellaneous lessons learned and recommendations

- Some players complained that organising the event over a weekend would have allowed them more involvement in the competition.
- Some players complained about the lack of prizes/stakes, sometimes stating that this was one of the main reasons for limited numbers of players representing their countries.
- Some players recommended not reusing challenges in future.
- Some players complained that participation by women needed to be considerably increased.
- The consortium recommends considering the possibility of (distributed) denial of service attacks on the infrastructure (the CTF platform and the challenges infrastructure) when creating such events, especially competitions with publicly available access, and enabling various security measures including:
    - backup infrastructure;
    - anti-denial of service attack solutions (e.g. websites should have Cloudflare or other traffic-filtering technologies in place);
    - auto-scaling infrastructures to address higher loads;
    - available response teams that can monitor the load and/or attacks and can respond properly in minutes;
    - dedicated resources for each player or for a number of players;
    - controlling access to infrastructures with tunnelling technologies such as OpenVPN/Wireguard.

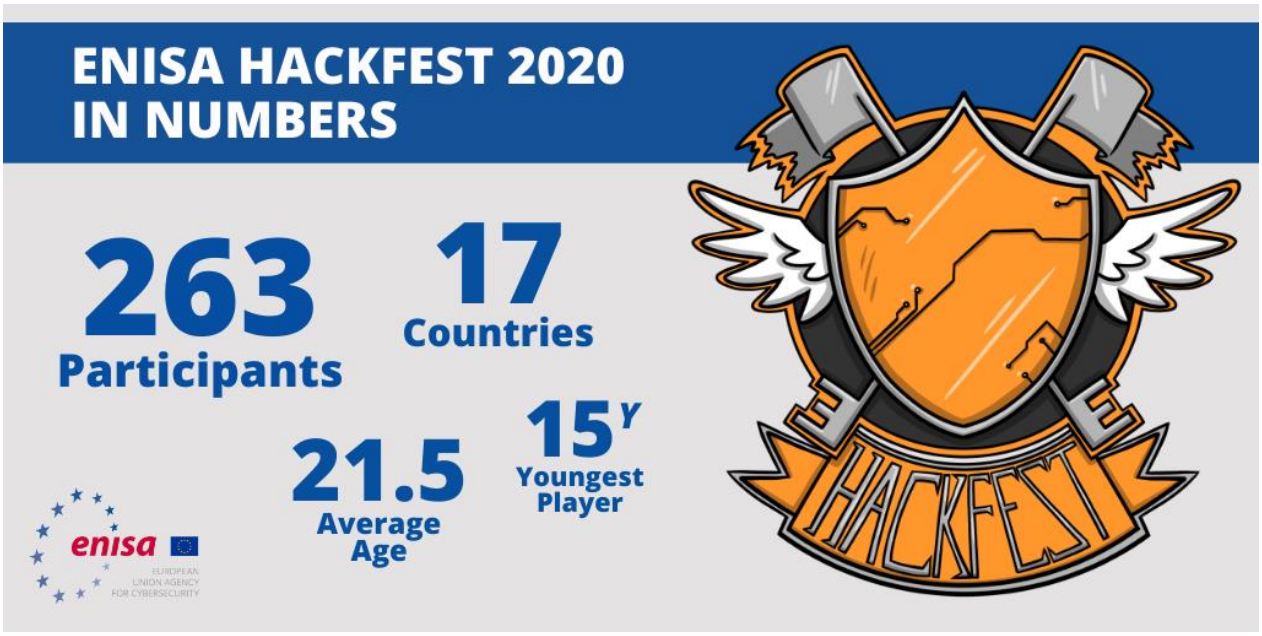
3.5.11. Public affairs and communications

After the competition, ENISA created and sent to the ECSC mailing list a document intended to align communication activities with all media points of contacts in the various ECSC participant countries.

The document contained the following information:

- links and guidelines on sharing information (text, hashtags, etc.),
- a link to an ENISA news item (https://www.enisa.europa.eu/news/enisa-news/enisa2019s-48h-hackfest-puts-europe2019s-cybersecurity-talent-to-the-test),
- social media links:
    - Twitter post 1 (https://twitter.com/enisa_eu/status/1329365661928177664),
    - Twitter post 2 (https://twitter.com/enisa_eu/status/1329381551575019520),
    - Twitter post 3 (https://twitter.com/enisa_eu/status/1329381843263746048/photo/1),
    - Facebook post (https://www.facebook.com/ENISAEUAGENCY/posts/3108688432569452), LinkedIn post (https://www.linkedin.com/posts/european-union-agency-for-cybersecurity-enisa_enisahackfest-cybersecurity-eu-activity-6735131891386658816-g3wi),
- statistics (some general information about the participation in the event),
- the competition logo,
- a screenshot of the platform,
- visual material for social media, developed by ENISA's public affairs team, as shown in Figure 5.

Figure 5: Social media material on ENISA Hackfest 2020



3.6. PLATFORMS

The updated list of ECSC-related platforms is the following:

- test scoreboard and contracts platform (only available from a certain point before the competition) (https://board.ecsc.eu),
- test scoreboard code repository (https://github.com/enisaeu/ecsc-gameboard),
- file-sharing platform (ownCloud) used for information sharing and as a contingency mechanism (https://storage.ecsc.eu/),
- the ECSC website used to promote the event and provide real-time scoring information during the challenge to external interested parties (https://www.europeancybersecuritychallenge.eu/),

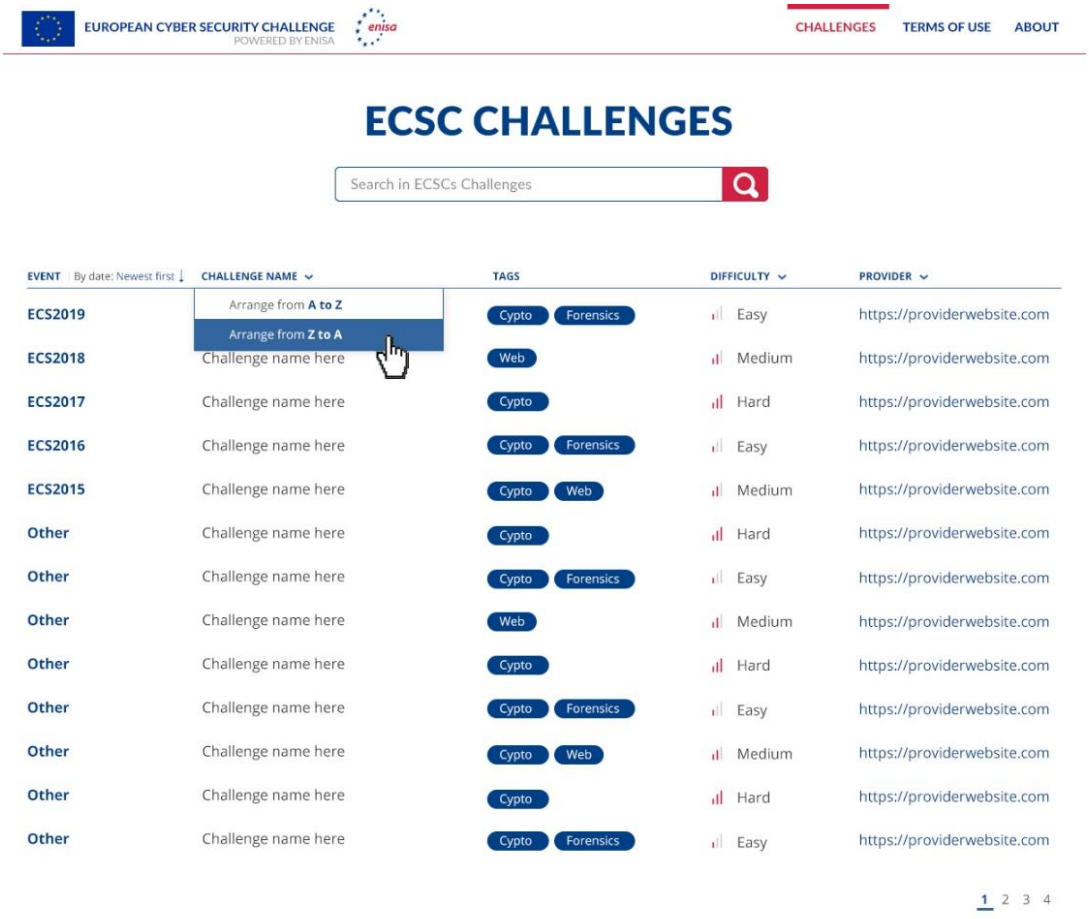
- the challenges platform on which previous years' ECSC challenges are collected (https://challenges.ecsc.eu/),
- the collaboration platform (https://cermit.enisa.europa.eu/ui/welcome).

During 2020, two new platforms were added to support ECSC activities, the ECSC challenges platform and the collaboration platform.

3.6.1. ECSC challenges platform

The idea was to create a simple, public-facing platform to provide access to all the challenges from past ECSCs and others that were not used during past events and could be used for training.

Figure 6: The ECSC challenges repository

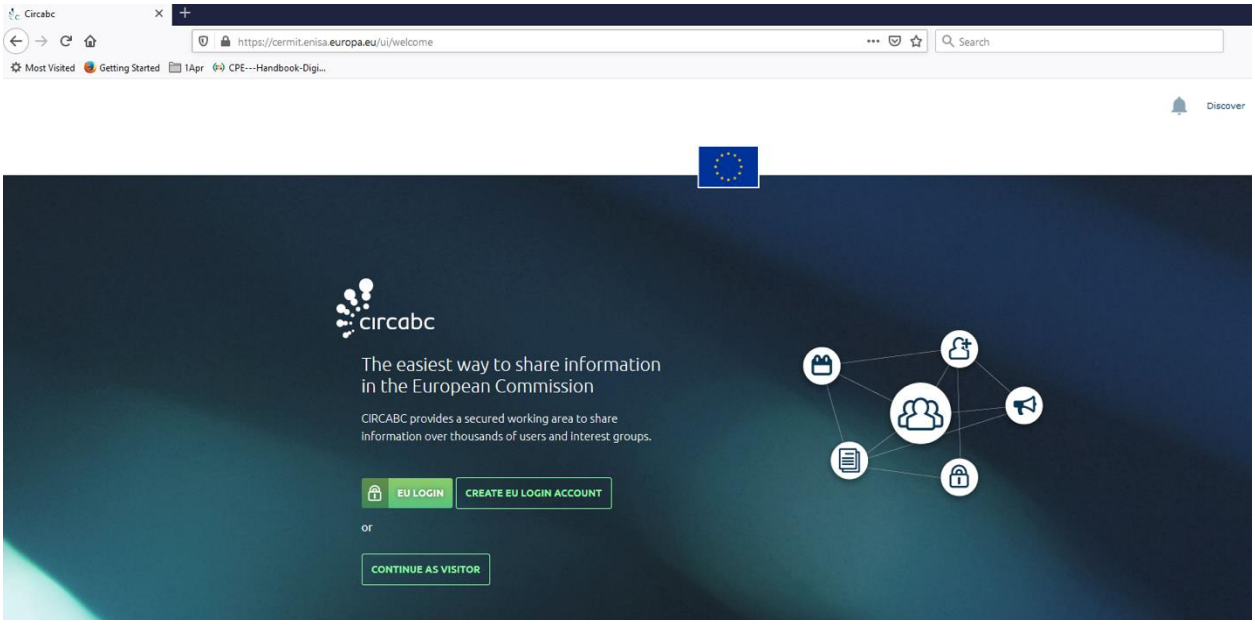


3.6.2. ECSC collaboration platform

The objectives of this platform are to improve the exchange of information among ECSC Steering Committee members and to provide a single place to store all ECSC-related information.

The selected platform, Cermit/CIRCABC, is supported and maintained by the European Commission and uses the European Commission Authentication Service (ECAS) as an authentication service.

Figure 7: The ECSC collaboration platform



3.7. Public affairs and media activities

The following key media activities were carried out during 2020 in collaboration with the various media points of contact appointed from the ECSC Steering Committee:

- coordinating the communication of the cancellation of the ECSC 2020 final,
- coordinating the announcement of the ENISA Hackfest 2020 post-event activities,
- updating attendees at the ECSC hot-wash meeting on ECSC public affairs activities.

Figure 8: Update on ECSC public affairs activities presented at the ECSC hot-wash meeting

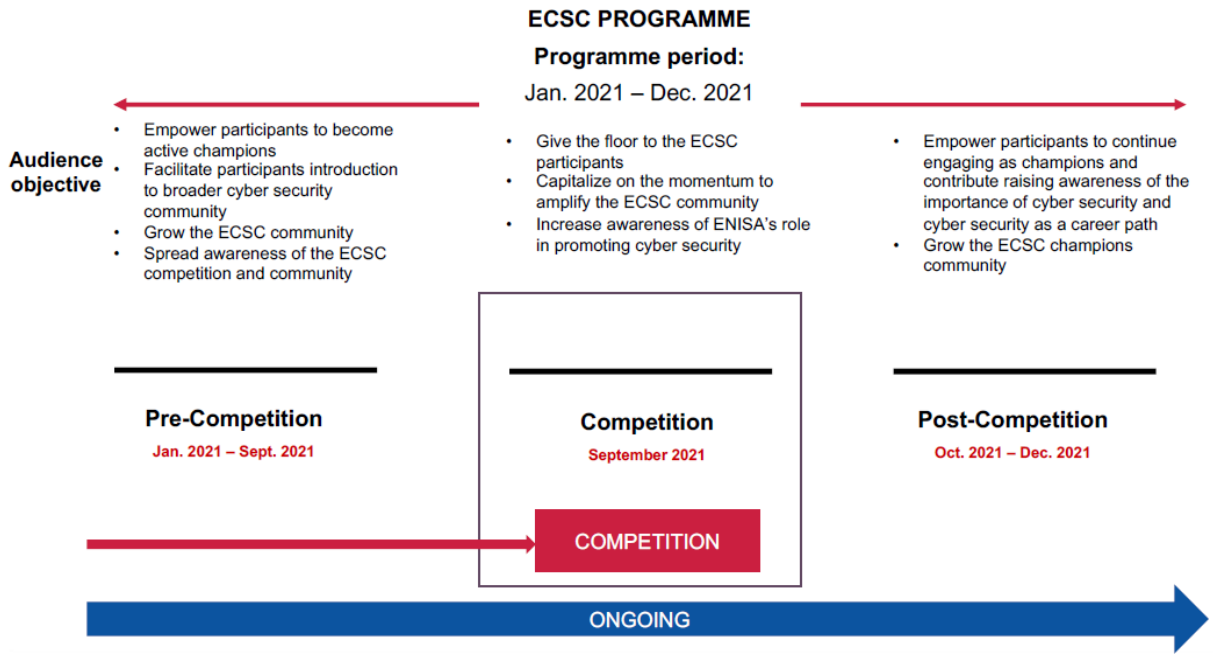
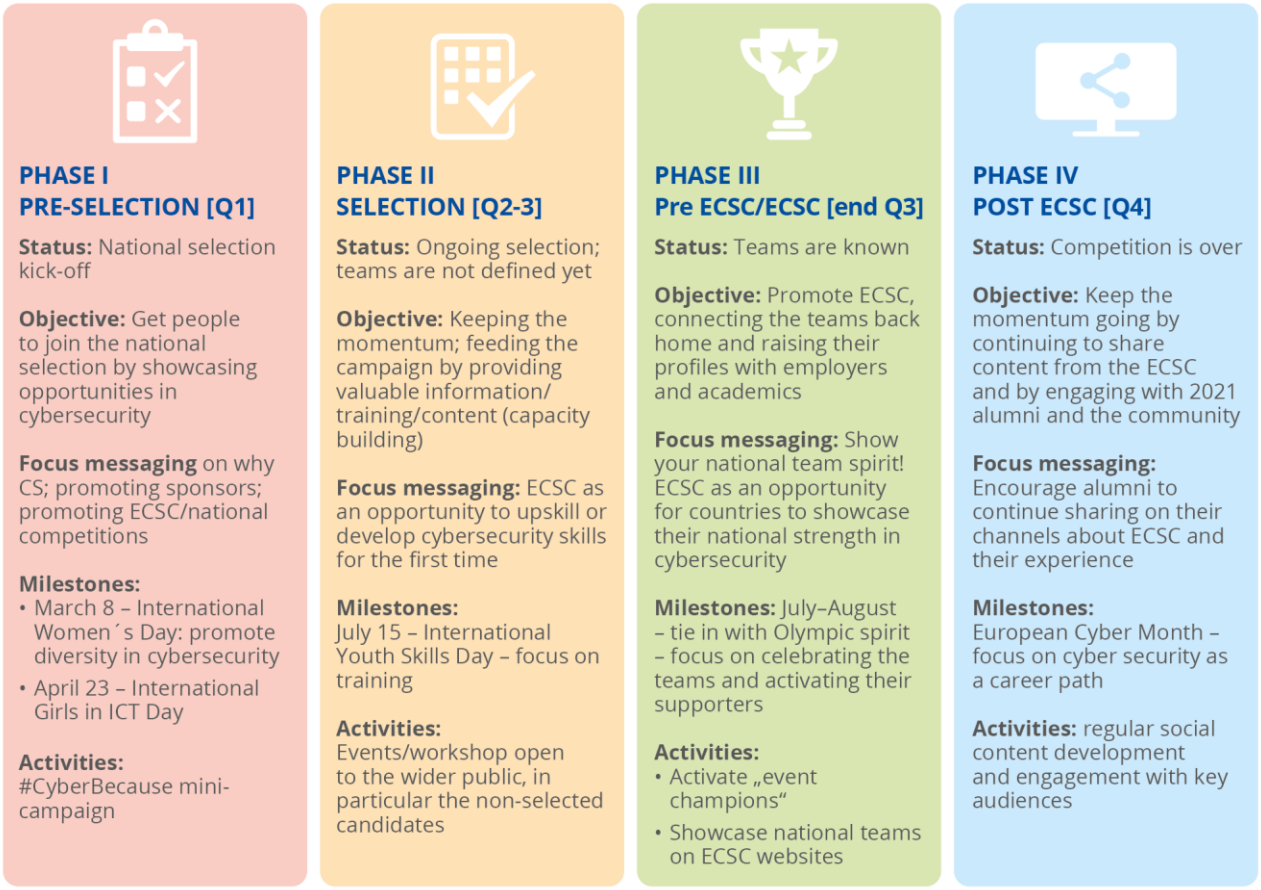


Figure 9: Phases of ECSC public affairs activities



3.8. WORKING GROUPS

During 2020, three new working groups were created, two of them as per the ECSC Steering Committee's decision during the initial planning conference in Vienna.

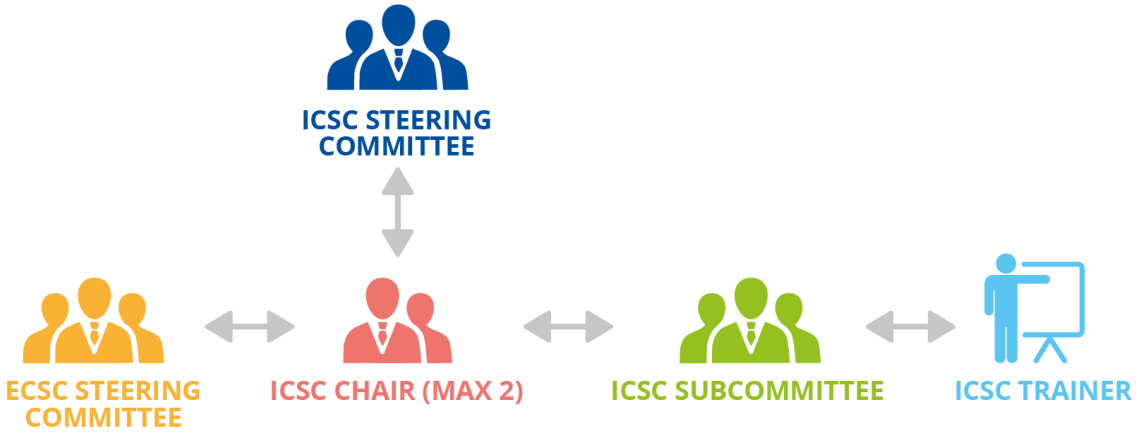
3.8.1. International working group

This group is intended to support the creation of Team Europe for the ICSC, planned for December 2021. During 2020, it carried out the following actions.

- The working group created the mandate for the ICSC Subcommittee, which was approved by the ECSC Steering Committee on 20 July 2020. The aim of the document is to set out the delegation of responsibilities from the ECSC Steering Committee to the subcommittee, and in particular to specify:
    - the composition and the means of acceptance of the subcommittee;
    - the tasks, purpose, role, boundaries and responsibilities of the subcommittee;
    - the duration of the subcommittee's mandate and the means of renewal.
- It created a document on the trainer selection process ('Coaches requirements and selection'), which was approved by the ECSC Steering Committee on 20 November 2020. The aim of the document is to set out the process for selecting the trainers for the future Team Europe, and in particular to specify:
    - the composition of the team of trainers and the means of selection;
    - the goals for Team Europe;
    - requirements for the trainers;
    - tasks, role, boundaries and responsibilities of the trainers;
    - the selection process;
    - the duration of the trainers´ mandate and the means of renewal.

- The working group created the call for trainers, launched on 23 November 2020.
- It proceeded with the final selection of trainers, which was completed on 11 December 2020.
- It started discussions about the selection mechanisms and the training path, in coordination with ENISA.

Figure 10: Relations between the international and European committees



3.8.2. Soft skills development working group

This working group was created to discuss and propose new ideas to replace the presentations as a soft skills development mechanism during the finals.

A space on the collaboration platform was created for this group; however, owing to the COVID-19 pandemic and the cancellation of the 2020 edition, no relevant decisions were made on this topic.

3.8.3. Media and public affairs points of contact working group

This working group was created to address the identified need to establish a permanent coordination group for the alignment of public affairs, communication and media activities.

This list of contact points is expected to improve timeliness and collaboration with regard to communication activities.

The group was started to work on the communication of the cancellation of the 2020 final and on communication activities relating to ENISA Hackfest 2020.

4. ECSC 2020 – LESSONS LEARNED AND MATURITY ASSESSMENT

A report on lessons learned has been produced by an external contractor on behalf of ENISA. It builds to some extent on the report on lessons learned from ECSC 2019, for the sake of consistency, and highlights comments and views provided by a number of ECSC Steering Committee members and ECSC representatives recommended by ENISA, as well as by several ENISA Hackfest 2020 organisers and participants.

Figure 10: Process of building the lessons learned

The report aggregates and puts into perspective a number of comments and views from stakeholders who were prompted to reflect on Hackfest 2020 and on the maturity of the ECSC. This feedback was collected through the following methods.

- Two online EUSurvey-based questionnaires, which combined closed and open-ended questions, and which were intended respectively for participants in Hackfest 2020 (defined as the individuals who were selected at national level and joined the event to try to solve the challenges) and for the organisers of Hackfest 2020 (understood in a generic way and referring to the people behind the organisation of the Hackfest event, including ECSC Steering Committee members). In total, 56 people responded to the questionnaires, distributed as follows: 47 participants and 9 organisers.
- A series of phone, Microsoft Teams or GoToMeeting interviews with ECSC Steering Committee members (or ECSC representatives acting as deputies) recommended by ENISA. In total, six interviews with eight people were conducted.

It is important to note that ENISA acted only as an intermediary in the data collection process. It provided support to encourage participation in the surveys and helped in identifying ECSC Steering Committee members to contact, but it refrained from any participation in the interviews in order to ensure the neutrality of the discussion.

Although the intention was to replicate the approach and methodology adopted for the maturity assessment conducted in 2019, the focus of which was ECSC 2019 (held in Bucharest, Romania), this report on lessons learned had to introduce some changes to the methodology owing to the specific circumstances caused by the COVID-19 pandemic, namely:

- no field research or direct observation-based inputs as part of the collected qualitative data;
- revision of the high-level domains because of the irrelevance of those related to venue and logistics;
- revision of some of the objectives to account for the change in event (Hackfest 2020 instead of ECSC 2020);
- adoption of a distinction between a general perspective (still appropriate for governance and decision-making and public affairs high-level domains) and a focus on Hackfest 2020 (for challenges and compliance).

For the sake of consistency, the high-level domains, parameters and evaluation criteria previously defined have been kept for this report. The change of scope, with Hackfest 2020 replacing ECSC 2020, has, however, rendered it impossible to conduct a maturity assessment directly comparable to the 2019 maturity assessment.

The following domains were evaluated:

1. governance and decision-making aspects,
2. public affairs – general perspective,
3. challenges – focus on Hackfest 2020,
4. logistics – aspects of the competition related to the venue, catering, hotels, transportation, etc.,
5. side events – aspects of the competition related to social events and networking meetings,
6. compliance – aspects of the competition related to compliance with laws and standards.

4.1. GOVERNANCE AND DECISION-MAKING ASPECTS

Parameter	Objective	Feedback from Hackfest / maturity assessment, questionnaires and interviews
Roles and responsibilities	An ECSC project governance model is established, which specifies that a dedicated team is to be established to organise the ECSC. This model includes clear roles and responsibilities to facilitate the correct ownership of tasks and project management.	• The presentation of the ECSC 2021 organisation team at the hot-wash meeting on 26 November 2020 was very useful. Some participants were pleasantly surprised that logistics-related aspects had already tackled and were reported on at this stage. • The hot-wash meeting on the last day of ECSC 2019 made the ECSC Steering Committee members realise that the Romanian organisational team had been relatively small and that each member of the organisational team had had a lot of responsibilities. The ECSC 2021 organisational team has been put together to ensure that the workload remains manageable for each team member. The decision has also been made by the Czech organisers that each team member is to be the coordinator of his or her own tasks, with clear prioritisation of tasks. • The Czech organisational team has adopted a 'crisis management' approach and has started thinking about potential problems that may arise and how to deal with them in a timely manner.
Decision-making of the ECSC Steering Committee and jury	The ECSC Steering Committee is a decision-making body that serves the improvement of the ECSC. Meetings of the committee are highly effective and have a clear and agreed-upon agenda. Decisions taken by the ECSC Steering Committee are logged in a decision-making register that can be referred to in subsequent meetings. This logbook contains information about decisions, owners and actions.	• A steering committee of 27 members is challenging. The ECSC Steering Committee nevertheless operates in a clear way and works towards improvements, concerned with learning from the past to make the next edition better. • Based on the responses to the organisers' questionnaire, 77 % of respondents consider that the ECSC Steering Committee performs well. • Suggestions for improvements are openly discussed within the committee and then followed up on. • There is no need for the ECSC Steering Committee to do things very differently. Some improvements could be made to accelerate the circulation of official documents when finalised and to clearly state who is to receive ECSC-related documents, for example everyone, ECSC participants or the members of the ECSC Steering Committee. • There is a good feeling that there are no hidden agendas within the ECSC Steering Committee and that committee members are willing to discuss and sort out any potential issues. • Concerning the way in which the 2020 cancellation was managed, it was stressed that the transparency shown by ENISA and its involvement of the ECSC Steering Committee in the decision-making were good. Decisions were made in agreement with all countries concerned, for example on how to communicate the cancellation of ECSC 2020. • It is helpful to have the CIRCABC as a centralised source of information.

Transparency	Decisions taken by the ECSC Steering Committee are communicated in a transparent manner to all relevant stakeholders including participants and organisers. Clear guidelines on the practicalities of the event are communicated to the audience in a timely manner.	• It is important that jury members be selected in a straightforward and transparent way. The jury selection process as designed and led by ENISA is efficient. • In addition to a clear division of labour and of roles and responsibilities, there is a need for ENISA and the ECSC hosting country to coordinate their communication and align the information they deliver to participants. • The model according to which the ECSC organiser takes the chair makes sense and has proved a good governance model. • The decision adopted for ECSC 2019 to have a jury making decisions then communicating them to the ECSC Steering Committee should be replicated, as it ensures unbiased decisions. • It was deemed by organisers that all the questions they raised about Hackfest 2020 received a timely and helpful response from ENISA.
National participation	As ECSC relates to European strategic policy objectives, the ECSC Steering Committee actively attracts and encourages non-participating European countries to become part of the initiative.	• There is value in having an increased number of participating countries. • Certain limitations need to be kept in mind, such as the logistical burden, costs for the hosting country, constraints on selecting an appropriate platform. • Since 2017, the ECSC has attracted more professionals and more countries. This has resulted in greater costs, a heavy logistical burden and funding-related issues. There is also a risk that the spirit of competition will prevails over the intended spirit of fun.

4.2. PUBLIC AFFAIRS – GENERAL PERSPECTIVE

Parameter	Objective	Feedback from Hackfest / maturity assessment and questionnaires
Monitoring, measurement and analysis (key performance indicators (KPIs))	In order to measure the effectiveness of the public affairs strategy, KPIs are set. These KPIs make it possible to monitor the impact of communication activities on the general public, measure the strategy's success in accordance with the objectives set and analyse the overall outcome of the strategy. In addition, this objective- and data-driven approach to assessing the activities conducted under the public affairs strategy make it possible to compare strategies over the years and identify trends.	• For guidance, participating teams need to be aware of the KPIs set out in the public affairs strategy. Collecting social media statistics from them should be feasible.

Dissemination plan	An ECSC dissemination plan is established in order to facilitate timely and coordinated implementation of the ECSC public affairs strategy among all participants and ECSC stakeholders. The plan ensures coherent and synchronised communication about ECSC in accordance with a well-defined dissemination timeline.	• The clear dissemination plan is helpful, but there is also a need to establish a transmission channel between the ECSC public affairs team and contractor on the one side and national teams on the other • Finding the right contact point in each country can be an issue. • ECSC provides a good dissemination plan and tools. However, some countries do not have sufficient resources to promote ECSC at national level or are not forceful enough in doing so. • To ensure consistent communication about ECSC, 'ready to post' messages should be prepared and communicated in advance when possible. • Special efforts should be put into the crafting of short sentences to make their translation from English into the participants' languages and the hosting country's national language easy. • Presenting all the ECSC 2021 participating teams in a soccer tournament-style graphic could be seen as a coherent and synchronised communication activity. This would enhance the ECSC's visual identity and underline the pan-European spirit of the event. • Communication during the challenges has to be very dynamic (e.g. live streaming). It should target the people who are not participating, since ECSC participants are very engaged anyway.
Key Messages	Targeted and effective key messages are developed to promote / communicate about the ECSC to all participants and ECSC stakeholders. The key messages are tailored to the different audiences (i.e. key audience, keep informed, keep satisfied, monitor) and dissemination phases (i.e. awareness, understanding, excitement, commitment, satisfaction).	• Many ECSC participants, especially those that do not have dedicated resources for communication activities, would welcome messages and communication materials crafted at ECSC level. This should include infographics and other visual elements to help to ensure that posts on Twitter or on participants' websites are eye-catching and engaging. • ECSC communication materials need to be easy to customise and to integrate into participants' own communication channels. • Using centralised/standardised communication materials has some limitations, especially when communicating with young people. Communication that is too official may be badly received, or not received at all, and could be detrimental to the 'fun competition' image that the ESCS is expected to convey. • There are differences between the way countries communicate (e.g. between northern and southern European countries). Centralised communication messages should be 'basic' enough to allow for cultural twists. • ECSC messages are more difficult to relay through national print media, as press articles cannot focus only on the competition. These messages have to include a reminder about what the ECSC is about in addition to adopting a clear national focus. • ECSC participants are likely to lack connections in the European print media and cannot be always expected to relay ECSC communication messages in this way.
Engagement and reach	The ECSC public affairs strategy is designed in such a way as to achieve maximum engagement of the audience. In order to sculpt the most relevant messages and maximise the interest and engagement of the audience, different engagement groups have been identified (i.e. key audience, keep informed, keep satisfied, monitor).	• Media influencers could be a good idea, but payment for them may be an issue. • Some organisations have embedded media influencers (e.g. a community manager). The issue at stake in this case relates more to alignment and coordination between participating countries. • Some channels are already well followed and YouTubers on cybersecurity would be great media influencers. • Having well-known female researchers in cyber active on Twitter and relaying messages about the ECSC would be helpful to attract more girls. • More media visibility is needed to improve all the teams.

Social media and visibility	Social media platforms (Twitter, LinkedIn, Instagram, Facebook) are used to facilitate interaction and dissemination of key messages with limited effort. Social media messages should be short, tailored to the audience and follow the dissemination plan in order to reach their full potential.	• There should be specific communication channels for ECSC, not only communication through ENISA's channels. • Specific ECSC LinkedIn, Twitter, Facebook and Instagram accounts are a step in the right direction. They will generate content that is easy to circulate and should trigger more interaction. • There is uncertainty about whether creating ECSC LinkedIn, Twitter, Facebook and Instagram accounts will be useful in teasing out and attracting new participants. YouTube might have greater reach. • Dedicated ECSC social media channels would make it possible to give more visibility to participating countries' posts, as ENISA cannot be expected to focus only on ECSC. • Dedicated ECSC social media channels would help centralise information and keep it up to date. • The fact that it is up to the hosting country and organisers to set up dedicated ECSC social media channels may mean that the ECSC misses out on benefits because of a lack of cumulative effects. Having permanent ECSC social media accounts would raise issues about ownership, though. • An explicit ECSC social media identity would increase the ECSC's visibility.
Website	An official ECSC website is set up to publish news updates (e.g. press releases) before, during and after the ECSC. The website allows the audience to replicate published messages and share them with other websites.	• The official ECSC website provides clear and informative content. • The redesign of the website after ECSC 2018 was well done and the site for ECSC 2019 offered better ergonomics and richer content. • Using the ECSC website to post news updates that are easy for participants to replicate and circulate should be helpful, especially if these updates include real-time information on the scoreboard.

4.3. CHALLENGES – FOCUS ON ENISA HACKFEST 2020

Parameter	Objective	Feedback from Hackfest / maturity assessment and questionnaires
Design	The design of the challenges reflects a reasonable learning curve in accordance with the average level of the participants. The challenges include real-life scenarios, which involve multiple aspects of cybersecurity and push participants to their limits.	• Based on the questionnaire sent to participants, 56 % of respondents did not find, or found only to some extent, the challenges diverse enough and requiring different skills. • There was an unbalanced number of challenges per category (e.g. there was only one exploiting challenge) and, generally speaking, too much web hacking. • Challenges that were a matter of guessing a certain method or approach, relying on random algorithms, were not considered good teaching material. • Forensics challenges that were more about steganography and random miscellaneous concepts than real-life forensic techniques were considered less interesting from a teaching perspective. • Steganography was commented on as not a valid CTF category in timed events, as, at most, it evaluates the users' creative insights and analytical skills. • Challenges should test participants' understanding of computers, not the creators' mindset or general knowledge of trivia. • Easier warm-up challenges were lacking and would have kept motivation high. • Challenges were lacking an intermediate waypoint to let participants know that they were on the right track. • Social skills were not really tested. • Solo participation instead of doing a CTF challenge as a team was considered far less fun and not as good from a learning

		perspective. It was also suspected to discourage participation in Hackfest 2020, as there are other online places that permit participants to tackle challenges with friends. • Prizes or goody bags would have been nice, as they are expected when participating in CTF competitions.
Rules	The rules are clear, unambiguous and agreed upon by all participants. The rules are clearly communicated to the teams. Compliance with the rules is monitored and used to avoid malicious activities.	• There was good awareness about the Hackfest rules among the participants. • Participants knew whom to approach with questions or if they had technical difficulties. • The overall process of qualification was unclear without concrete rules on how Hackfest 2020 related to qualifying competitions.
Enforcement	The rules are enforced in a consistent manner. Breaches of the rules are followed by the consequences are agreed upon by the jury.	• Some participants noticed that at some point during the CTF competition more than 20 people were in the Discord voice chat exchanging flags. • It was very difficult to judge whether some participants did or did not use existing write-ups in their solutions to challenges.
Presentations **(NB: this parameter relates specifically to the ECSC)**	The content of presentations given by participants and/or sponsors aligns with the objectives of the ECSC regarding building expertise and meets the expectations of participants.	• The team presentation at the ECSC is deemed a challenge in itself. • The jury's expectations are unclear, and this makes it difficult for people presenting to pitch for the right audience; they run the risk of being too technical (or not technical enough).
Platform	A capacity and quality assessment of the platform is performed to ensure the stability and security of the platform during the challenge and its ongoing ability to meet the requirements, standards, scale and expectations of the ECSC. Unforeseen circumstances that might affect the continuity of the platform – and of the event – are thereby taken into account. The assessment of the platform includes regular and adequate testing of the platform by the service provider.	• Based on the questionnaire sent to participants, 76 % of respondents considered that the performance of the platform was good or excellent. • The platform was considered reliable and stable, with good support provided by the Bit Sentinel team.
Infrastructure	The IT infrastructure supporting the platform for the ECSC is reliable, trustworthy and ensures all participants can equally and fairly connect to the platform. The infrastructure provider should take into account potential unforeseen circumstances that might affect the continuity of the infrastructure and take preventive and reactive measures as appropriate (including failovers, backup configurations, high-availability measures).	• No major issues or incidents with regard to the availability of network infrastructure were reported by respondents to questionnaire and interviewees. • The registration process could have been more straightforward, according to some participants, but in general, it was deemed fine.
Complexity	The level of complexity of the challenge is sufficiently mature to provide a challenging competition that attracts top cybersecurity talent from all over Europe. The complexity meets the participants' expectations.	• Based on the questionnaire sent to participants, 34 % of respondents were satisfied to some extent by the technical complexity of the challenges and 30 % were not. • Some challenges were considered fun but, in general, participants felt that the challenges were not of the quality expected of such an event. In particular, the reuse of several challenges, write-ups on which were already widely available online (e.g. from DefCamp Capture the Flag 2019), was disappointing to them.

		• Participants who were familiar with CyberEDU or the DefCamp 2019 competition were perceived as having a slight advantage. • In addition to challenges that were re-used, those involving too much guessing were deemed 'unfair' and even to ruin part of the fun. • Some participants noticed spelling mistakes. • Challenges involving Braille, Morse code or guessing were criticised by some participants. • Brute-forcing as an intended solution to recover a flag was not deemed a good thing. Where a task had a good back story but some cipher (considered 'obscure') was put on the flag when all the other parts of the task had been solved, ending the challenge in this way was not considered enjoyable. • Hints should have been more useful and more numerous. • From a practical point of view, it was regretted that the Hackfest had taken place during the week. As the participants were mostly students and young professionals, it was difficult for them to free themselves up to participate fully. This factor alone limited the level of participation in Hackfest 2020 and led to some participants thinking they had been at a disadvantage. • Holding an event during the working week makes it more difficult to guarantee that all the participants from all countries have the same availability to compete.
Scoring	The scoring mechanism is transparent with regard to attribution and distribution of points and is approved by the ECSC Steering Committee.	• The lack of a global scoreboard, making it impossible for participants to compare their performance against others, was considered an issue. • The scoring method was not clear. • Some participants resented the fact that dynamic scoring was mixed with so many challenges that required guessing, so that some challenges that required a huge amount of work and competence were worth less than some challenges that were not instructive. • The scoreboard seemed to be not completely fair. • A lack of opportunities for participants to receive some feedback on how well they perform is likely to reduce the incentive to participate, especially in the case of solo CTF challenges.

4.4. COMPLIANCE – FOCUS ON ENISA HACKFEST 2020

Parameter	Objective	Observations
Data protection	The ECSC Steering Committee is committed to ensuring compliance with relevant data protection and privacy legislation such as the general data protection regulation. Although the ECSC does not process personal data as part of its core business, it may happen that some activities require processing of personal data (e.g. collecting customer satisfaction information or publishing pictures of the event)	• The requirement to have a Google account for submitting write-ups, especially when having a registered account on the CyberEDU platform already, was puzzling to some participants. • Some participants did not like that documents were shared on Google Drive. • Some participants found it weird to have to give their full name and that it was displayed on the scoreboard. They were expecting that usernames would be enough. • An issue was reported on the Discord server. The ticket to access a dedicated page was not clearly communicated and some participants found themselves receiving messages from other events going on at the same time.

5. AREAS FOR IMPROVEMENT AND RECOMMENDATIONS

5.1. GOVERNANCE AND DECISION-MAKING ASPECTS

Parameter	Recommendations
Roles and responsibilities	• National teams should be made aware of the amount of work involved in the preparation for and organisation of ECSC events, to manage expectations. • National team members should be encouraged and reminded to respond to the survey circulated by the Czech organisers, in order to help them anticipate as much as possible participants' needs and facilitate their work.
Decision-making of the ECSC Steering Committee and jury	• Ensure that all ECSC 2021 participants are aware that the Czech national team will not take part in the competition, to end any potential concerns about the national team's having some undue advantages. • Make the most of the CIRCABC platform, ensuring that all the ECSC Steering Committee members who were experiencing issues with logging in have sorted them out and that news, the committee's agendas, minutes and related documents are uploaded in a timely manner and kept up to date on the platform. • The decision-making process adopted in Romania, with the jury taking decisions then passing them on to the ECSC Steering Committee, should be retained, as it proved to be efficient.
Transparency	• Make sure that the recipients to be sent ECSC-related documents are explicitly mentioned in the documents, to facilitate their circulation. • Clarify the relationship between the ECSC and ICSC steering committees and have more meetings minuted to avoid any misunderstandings or misinterpretations that could lead to confusion among the ECSC Steering Committee members.
National participation	• Concerns voiced by some ECSC members that by expanding to new countries, logistics- and funding-related issues have grown to the point that they are compromising the ECSC's spirit of fun should be taken into account and addressed.

5.2. PUBLIC AFFAIRS – GENERAL PERSPECTIVE

Parameter	Recommendations
Monitoring, measurement and analysis (KPIs)	• Inform participating teams in advance that social media statistics will be collected from them by public affairs personnel and start thinking about an easy and straightforward way of doing that.
Dissemination plan	• Make sure that participating teams are well aware of the dissemination plan, for example by organising a brief dedicated videoconference during which ENISA's public affairs team and contractor present the key aspects of the dissemination plan to participating teams. • Provide some guidance about social media and communication. • Incentivise participating teams to jointly disseminate information with combined messages, for example through the establishment of a top three or top five ranking of the most active participating teams, to be made public at the end of the event (with a prize, if possible).

Key messages	• Ensure that the pan-European spirit of the ECSC is well reflected in the communication messages, to appeal to the collaborative mindset of the participating teams and convey clearly the European identity of the ECSC. This would be well received by participants, who sometimes feel like the 'E' is missing in 'ECSC'. • Develop ECSC-specific and easy to customise digital media content, including graphic elements such as infographics and appealing visuals for publication on social media channels. • ENISA's public affairs team and contractor are to be responsible for liaison with the European print media, as they have connections that participating teams do not have. • Key messages should be crafted to attract more women.
Engagement and reach	• Identify ECSC members with connections with YouTubers active on cybersecurity-related topics or find a way to contact them and ask them for their support in raising awareness about the ECSC. • Identify potential ECSC members with connections with female researchers in cybersecurity active on social media, not only to raise awareness about the ECSC but also to attract more girls to the cybersecurity sector. • Make the most of the European Cybersecurity Month in October to promote the ECSC. • Reach out to schools and invite more students.
Social media and visibility	• Find a way to avoid starting from scratch when social media accounts are being created by the new ECSC organisers, to capitalise on the experience and good ideas of the organisers who launched the social media accounts the year before. • Explore possible solutions to deal with the ownership issue and make it possible to create a dedicated ECSC social media identity (e.g. on Twitter and LinkedIn) and strengthen the ECSC brand.
Website	• Ensure that the ECSC website is regularly updated to provide participants with all relevant information in a timely and accurate way. • Post dynamic content on the website (e.g. live streaming and live scoreboard information).

5.3. CHALLENGES – LESSONS LEARNED FROM ENISA HACKFEST 2020

Parameter	Recommendations
Design	• Ensure enough diversity in the challenges. • A 'very good challenge', according to one of the respondents to the participants' questionnaire would meet the following requirements: o very well designed o a learning experience o innovative o fair o fun. • Try to harmonise flags' formats, which can vary a lot depending on the supplier. • Enhance the cooperative mindset and the European 'branding'. • Small countries (e.g. the five smallest ones) should be allowed to cooperate against major teams. • Consider adding some boot2root challenges and create activities that members of teams from different countries are expected to collaborate on, instead of their having to compete against each other for the duration of the event. • Even if the event has to become virtual because of the COVID-19 pandemic, find ways to encourage interaction and collaboration.

Rules	• Implement a section on the ECSC platform that details the ECSC rules and the good conduct expected of the participants. • Find a way to display the Charter of Good Conduct during the event. • Something as simple as a terminology brief describing the roles, functions and responsibilities of the various people taking part in ECSC events could be helpful in making people aware of the rules, especially those that apply more particularly to them depending on their function (captains, coaches, trainers, qualifiers, organisers, etc.). • The choice of a channel for communication among participants should be made in advance and thought should be put into how communication will be structured (e.g. who should have access to what, which spaces should be created). Once it has been decided on, registration with the communication channel could be made compulsory.
Enforcement	• Identify a platform or a channel (within Discord, for instance) where an incident-reporting space could be created for participants to notify the jury of potential issues, such as cheating or unethical behaviour. • If using a Discord-type channel, check that participants do not use it to exchange flags. • Consider publishing exchanges on a Discord-type channel for transparency purposes.
Presentations **(NB: this parameter relates specifically to the ECSC)**	• Explain clearly what the requirements for the presentations are and what the level of technical expertise of the jury panel is. • Post an agenda giving the order and timing of the presentations on the ECSC platform and website.
Complexity	• Participants are more and more demanding about the quality and complexity of challenges and tend to expect that considerable thought and care will have been put into their creation, for example by forensics professionals. • Do not reuse challenges, to ensure that no write-ups are available. • Avoid challenges that involve guessing or that are not originals. • Create more education-oriented challenges. • Check carefully for misspellings.
Scoring	• Ensure that challenges that require a lot of work to find the solution are worth more than challenges that require guessing or random algorithms to be solved.

5.4. COMPLIANCE – LESSONS LEARNED FROM ENISA HACKFEST 2020

Parameter	Recommendations
Data protection	• Do not require participants to have a Google account to submit write-ups. • Do not display full names on the scoreboard.

6. ECSC 2021

The final of the 2021 edition of the ECSC will take place in Prague in September 2021; at least 22 countries are expected to participate. The latest updates will be published on the ECSC 2021 website (https://www.europeancybersecuritychallenge.eu/).

Figure 11: The ECSC 2021 logo

TP-03-21-123-EN-N

About ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found on its website 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: 978-92-9204-496-1
DOI: 10.2824/284260