



# ECSC 2019 ANALYSIS REPORT

Maturity Assessment and Lesson Learnt of the  
European Cyber Security Challenges 2019

DECEMBER 2019

# 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](http://www.enisa.europa.eu).

## CONTACT

For contacting the authors please use [ecsc@enisa.europa.eu](mailto:ecsc@enisa.europa.eu).

For media enquiries about this paper please use [press@enisa.europa.eu](mailto:press@enisa.europa.eu).

## AUTHORS

Adrián Belmonte Martín, ENISA

## ACKNOWLEDGEMENTS

We would like to thank our colleagues at ANSSI and CERT.RO for taking care of all local logistics for the organisation of ECSC'2019.

Finally, we would like to thank all our colleagues responsible for the national competitions and the preparation of the teams that participate at the ECSC. Without their untiring efforts this competition will not be possible.

## LEGAL NOTICE

Notice must be taken that this publication represents the views and interpretations of ENISA, unless stated otherwise. This publication should not be construed to be a legal action of ENISA or the ENISA bodies unless adopted pursuant to the Regulation (EU) No 2019/881.

This publication does not necessarily represent state-of-the-art and ENISA may update it from time to time.

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

This publication is intended for information purposes only. It must be accessible free of charge. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

## COPYRIGHT NOTICE

© European Union Agency for Cybersecurity (ENISA), 2019

Reproduction is authorised provided the source is acknowledged.



# TABLE OF CONTENTS

<b>1. INTRODUCTION</b>	<b>6</b>
1.1 ECSC BACKGROUND	6
1.2 ECSC SETUP	7
<b>2. ECSC ATTENDANCE EVOLUTION</b>	<b>8</b>
<b>3. ECSC 2019 HOSTING COUNTRY</b>	<b>9</b>
<b>4. ENISA CONTRIBUTION TO ECSC2019</b>	<b>10</b>
4.1 STEERING COMMITTEE MANAGEMENT	10
4.2 JURY MANAGEMENT	10
4.3 PRESENTATIONS MANAGEMENT	12
4.4 PLATFORMS	13
4.5 SCORING PLATFORM (SCORE BOARD)	13
4.5.1 The use of GitHub	14
4.6 ECSC NEW WEBSITE	16
4.7 COMPETITION CHALLENGES	16
4.8 PUBLIC AFFAIRS STRATEGY	18
4.8.1 Women in Cybersecurity in the context of the European Cybersecurity Challenge	18
4.9 GALA NIGHT SPEAKER	19
4.10 SOCIAL MEDIA IMPACT	20
4.11 CONTINUOUS IMPROVEMENT: IMPROVEMENTS TO THIS YEAR EDITIONS	20
<b>5. FINAL RESULTS</b>	<b>21</b>
5.1 POST EVENT ACTIVITIES	21
<b>6. LESSONS LEARNT</b>	<b>23</b>
6.1 GOVERNANCE AND DECISION-MAKING ASPECTS	23
6.2 PUBLIC AFFAIRS	24



<b>6.3 CHALLENGE</b>	<b>25</b>
<b>6.4 LOGISTICS</b>	<b>27</b>
<b>6.5 SIDE EVENTS</b>	<b>28</b>
<b>6.6 COMPLIANCE</b>	<b>28</b>
<b>7. MATURITY ASSESSMENT RESULTS</b>	<b>29</b>
<b>8. ECSC 2020</b>	<b>31</b>



# EXECUTIVE SUMMARY

The 6th Edition of the European Cyber Security Challenge, ECSC2019 was hosted in Bucharest during 9th to 11th October. The event was organised by ANSSI (Asociatia Nationala pentru Securitatea Sistemelor Informatice) and CERT.RO (Centrul national de raspuns la incidente de securitate cibernetica) at Palace of the Parliament.

Each country was represented at the ECSC final by a team of 10 contestants, comprised of the winners of the national competitions. Half of the team members are within the range of ages of 14-20 years old and half in the 21-25 range. In total, 300 people (contestants, coaches and judges) representing 20 EU and EFTA countries (Austria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland, United Kingdom) competed in the ECSC final in Bucharest. The participants investigated vulnerabilities in web applications, binaries and document files, solved crypto puzzles and hacked hardware systems. However, technical skills are just one part of the whole story. Teamwork and presentation skills were also evaluated. A significant part of the skillset, which is important for working in an IT security team, is thus tested. The finalists of ECSC 2019 were the teams from Romania, Italia and Austria.

ENISA is currently hosting different platforms and performing different activities to support the European Cyber Security Challenge hosting country and the evolution of the project, this includes among others: ECSC main website, ECSC planning platform, public affairs strategy, challenges creation, governance framework of the competition, secretariat support, etc...

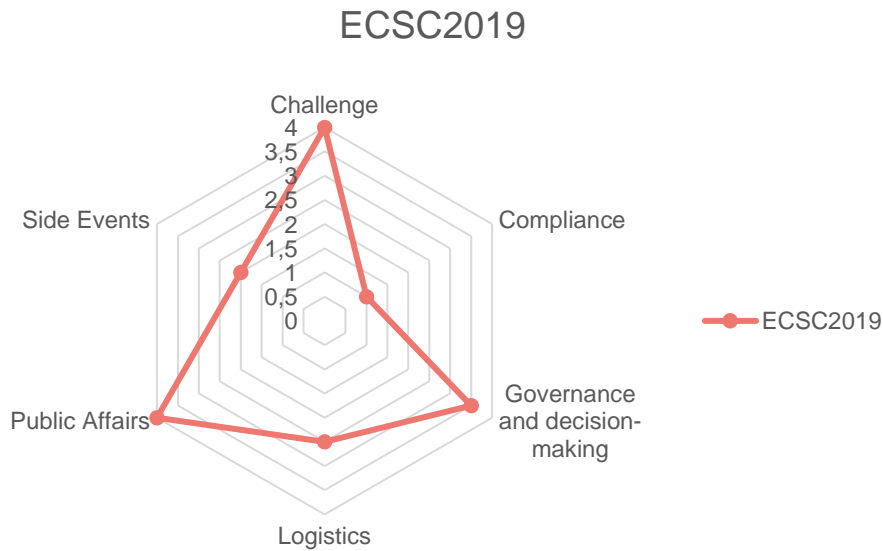
In order to ensure appropriate and transparent reporting to the Steering Committee, the following key observations were made by independent third-party observers that have attended the ECSC planning meetings and the actual event. These observations have been produced based on the feedback collected from participants, members of the ECSC Jury, members of the ECSC Steering Committee, and attendees to the event. In addition, these observations reflect the feedback provided by organisers and participants collected by an online evaluation survey:

- Roles and responsibilities were clearly defined and respected during ECSC planning meetings. The different organisational stakeholders and ECSC Steering Committee members were documented in an ECSC WhoisWho, which aimed at ensuring transparency about the individual stakeholders and their role in the competition.
- The total reach on social media for the #ECSC2019 campaign from February 1st, 2019 up until October 21st, 2019 is estimated at 1.2 million people and the total amount of mentions on social media is estimated at 2113. The total amount of interactions on social media is estimated at 22 240.
- The introduction of an independent jury body in the competition was considered a great achievement for this year edition.
- The participating teams have successfully adopted the key messages embedded in the ECSC Public Affairs Strategy. An increased level of activity by the national teams has been observed.
- The network infrastructure for the platform was reliable and stable. No major issues or incidents took place with regards to the availability of network infrastructure. Network capacity and speed was meeting expectations.

A maturity assessment on different areas was developed based on the feedback collected from participants, members of the ECSC Jury, members of the ECSC Steering Committee, and attendees to the event.

The graphical representation of the obtained values are the following:

**Figure 1: ECSC maturity assessment**



The 2020 edition of the European Cyber Security Challenge will take place Vienna Austria, in November 2020.

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 competition.

# 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<sup>1</sup> in order to be able to prevent, react and protect their citizens against cyber threats. Europe has to make an effort to retain and attract talent to cybersecurity and, at the same time, create solid and powerful education, entrepreneur and business structures on cyber security.

To help mitigate this shortage of skills, many countries launched national cyber security competitions addressed towards students, university graduates or even non-ICT professionals with a clear aim:

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

The European Cyber Security Challenge (ECSC) <https://www.europeancybersecuritychallenge.eu/> leverages on these competitions by adding a pan-European layer. Top cyber talents from each participating country meet to network and collaborate and finally compete against each other. Contestants are challenged in solving security related tasks from 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 cyber security. Its main aim is to highlight the importance of the national competition.

## 1.1 ECSC BACKGROUND

The project was initiated under the umbrella of the EU Cyber Security Strategy (Feb 2013):

*'The European Commission will organise, with the support of ENISA, a cybersecurity Championship in 2014, where university students will compete in proposing NIS solutions.'*

As of 2014, ENISA has been supporting the organisation of the ECSC. ENISA is actively organising the meetings of the governance structures, supporting the development of the competition rules and games and is part of the ECSC Jury. As of 2016, ENISA is the acting secretariat of the ECSC Steering Committee.

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

The 2019 edition of the European Cyber Security Challenge took place in the Parliament building in Bucharest, Romania, from 9th to 11th October 2019. For the first time, teams from 20 countries participated at the final (Austria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland, United Kingdom). The participants investigated vulnerabilities in web applications, binaries and document files, solved crypto puzzles and hack

**ECSC is the annual European event that brings together young talent from across Europe to have fun and compete in cyber security.**

<sup>1</sup> <https://www.forbes.com/sites/forbestechcouncil/2018/08/09/the-cybersecurity-talent-gap-is-an-industry-crisis>

hardware systems. However, technical skills are just one part of the whole story. As time and resources were limited, teamwork and presentation skills were also evaluated. The finalists of ECSC 2019 were the teams from Romania, Italy and Austria.

The 2020 edition of the European Cyber Security Challenge will take place Vienna, Austria between 3<sup>rd</sup> and 7<sup>th</sup> November

## 1.2 ECSC SETUP

Each country is represented at the ECSC final by a team of 10 contestants, comprised by the winners of the national round. Half of them are within the range of ages of 14-20 years old and half in the 21-25 range.

Two preparatory pilot phases of ECSC have been held in 2014 (in Austria) and 2015 (in Switzerland) with attendance by 3 and 6 countries, respectively. Since 2015, ENISA is lending its experience and position to coordinate and organise the ECSC effort to reach its full maturity by 2020.

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 different platforms and performing different activities to support the European Cyber Security Challenge hosting country and the evolution of the project, this includes among others: the ECSC main website, the ECSC information-sharing platform, the public affairs strategy, challenges creation, etc...

In addition, ENISA is working closely with the host of each edition, in order to ensure appropriate and transparent reporting to the Steering Committee.

During the year, two Steering Committee meetings are held prior the execution of the event:

- Initial Planning Conference (IPC), held in Bucharest, 6<sup>th</sup> -7<sup>th</sup> of March in DG Connect
- Main Planning Conference (MPC), held in Bucharest during 20<sup>th</sup>-21<sup>th</sup> of June

ENISA organised these preparatory events and was overall responsible for the efficient running of the project, including meetings minutes and the follow-up of the proposed actions.



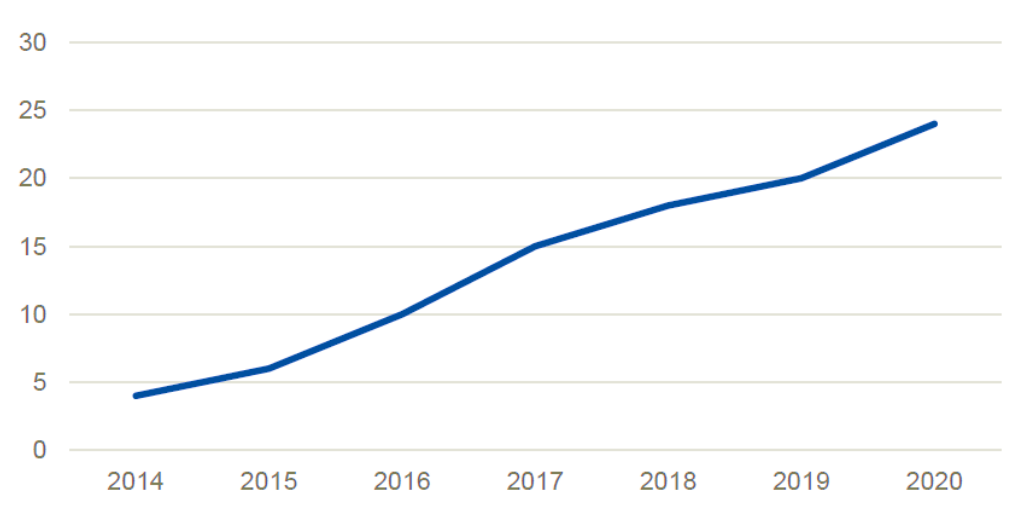
## 2. ECSC ATTENDANCE EVOLUTION

From the first edition of the ECSC in 2014 the evolution of the attendant's countries has been the following:

- 2014 [3]: Austria, Germany, Switzerland
- 2015 [6]: Austria, Germany, Switzerland, Spain, Romania, United Kingdom
- 2016 [10]: Austria, Estonia, Germany, Greece, Ireland, Liechtenstein, Romania, Spain, Switzerland, United Kingdom
- 2017 [15]: Austria, Cyprus, Czech Republic, Denmark, Estonia, Germany, Greece, Ireland, Italy, Liechtenstein, Norway, Romania, Spain, Switzerland, United Kingdom
- 2018 [17]: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Liechtenstein, Norway, Poland, Romania, Spain, Switzerland, United Kingdom
- 2019 [20]: Austria, Cyprus, Czech Republic, Denmark, Estonia, France, Germany, Greece, Italy, Ireland, Liechtenstein, Luxembourg, Netherlands, Norway, Poland, Portugal, Romania, Spain, Switzerland, United Kingdom

Figure 2, depicts the growth of the ECSC since the involvement of ENISA in the competition back in 2014.

**Figure 2: ECSC evolution in participation**



## 3. ECSC 2019 HOSTING COUNTRY

The 6th Edition of the European Cyber Security Challenge, ECSC2019 was hosted in Bucharest from 9th to 11th October. The event was organised by ANSSI (Asociatia Nationala pentru Securitatea Sistemelor Informatice) and CERT.RO (Centrul national de raspuns la incidente de securitate cibernetica) at Palace of the Parliament, the heaviest building in the world<sup>2</sup>.



Palace of the Parliament, Bucharest (Romania).

The organization provided different useful information about how to get to the event, a selection of recommended hotels and the different facilities provided during the execution of the competition. In addition, different activities were performed for the participants:

- Tuesday 8<sup>th</sup> Oct : Welcome dinner and presentation of the teams
- Wednesday 9<sup>th</sup> Oct: Dinner in Bucharest with some of the teams
- Thursday 10<sup>th</sup> Oct: ECSC2019 Competition Closing Party
- Friday 11<sup>th</sup> Oct: Awards ceremony and gala dinner at the Palace of the National Military Circle

---

<sup>2</sup> [https://en.wikipedia.org/wiki/Palace\\_of\\_the\\_Parliament](https://en.wikipedia.org/wiki/Palace_of_the_Parliament)

# 4. ENISA CONTRIBUTION TO ECSC2019

## 4.1 STEERING COMMITTEE MANAGEMENT

The activities of the ECSC are supervised by a Steering Committee (SC) 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 approved every year.

During the preparation of ECSC 2019, ENISA was responsible for the following activities related with the management of the Steering Committee:

- Platforms maintenance and update
- Mail list management
- Update and creation of SC related documentation
- Organization of the IPC in Brussels
- Support the organization of the MPC in Bucharest
- Accommodation, execution and follow-up of SC requests
- Implementation of changes and suggestions collected using surveys and the feedback from previous editions
- Creation and management of an independent jury
- Creation of an internal 'Who is who' document to support the jury and teams activities
- Realisation of a 'Comcheck' prior to the competition
- Organization of a Hot wash meeting after the execution of the competition in Bucharest
- Feedback collection: Lessons learnt report and surveys to the participants

## 4.2 JURY MANAGEMENT

The proposal for this year edition was the creation of an independent jury body, instead of the format of the previous editions of having 'jury members' appointed by each participating country. By Steering Committee decision, the independent jury was composed of 5 members: 3 independent + 2 members by the following organizing countries, Austria and Czech Republic

To guarantee the full transparency and the independency of the selection of Jury members, the procedure for selecting the jury was the following:

- ENISA opened a period to nominate candidates in order to collect as many potential candidates as possible. ENISA also contributed to the list by providing names from its stakeholders' lists.
- Creation of a list of candidates: The list is a living document and is updated/refreshed at regular intervals. After the release of each update, there is a period where any member of the SC has the right to exercise his/her reservations to any proposed candidate in the list.
- If a SC member decides to exercise the right to veto to any of the candidates in the list, the name will be removed after official communication.
- Once the final deadline for exercising the possibility of veto, the list of candidates is considered final. Any name in the list is considered equally eligible
- The final selection of candidates was done by ENISA who is also responsible for contacting the candidates and check for availability

- The final jury was kept in secret until the day of the competition, to avoid possible interferences or contacts with the jury members

The final composition of the jury was the following:

- Alex Zacharis: Security Engineer for the European Global Navigation Satellite Systems Agency (GSA).
- Simone Fisher: Professor at the Department of Computer Science at Karlstad University. Member of the Information Security Council at the Swedish Civil Contingencies Agency
- Mateusz Szymaniec: Security specialist at CERT Polska,
- Paul Varga: Teacher for IT Security at the university of applied sciences Technikum-Wien. Representative by Austria
- Petr Jirásek: AFCEA Regional Vice President for Central Eastern European and Baltic Region. Representative by Czech Republic

As for previous editions, the following activities related to jury management were carried out:

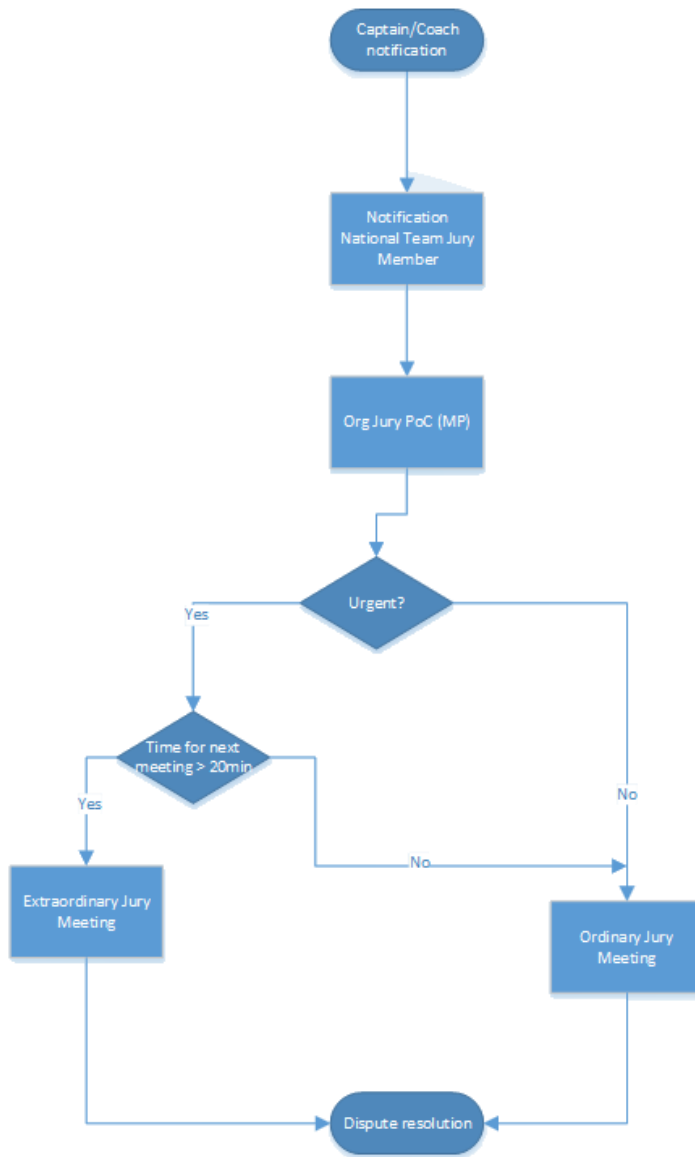
- An updated "Jury guidelines" document was populated, summing up the most important points to take in to account. The Jury members and captains from all teams could use this document as a reference.
- Jury meetings were scheduled at regular intervals in order to improve the efficiency of the competition: Jury members met at predefined times during the competition to discuss and resolve complaints and queries received during the period in between two jury meetings. In addition, a framework was created in the case an "extraordinary jury meeting" was necessary for issues that may affect severely the running of the competition.
- The jury coordinator: In charge of acting as a PoC, receiving and collecting complains from participants, captains and jury members.

In general, during the competition the role of the jury was:

- Attend jury meetings
- Resolve disputes with impartiality
- Attend and evaluate presentations
- Attend to any other issue that may need the expertise of the jury.

Definition of a clear workflow in case of complaints. The workflow is depicted in Fig. 3.

**Figure 3: ECSC Complaints to jury workflow**



### 4.3 PRESENTATIONS MANAGEMENT

For ECSC 2019, ENISA by SC decision updated and incorporated new guidelines and rules for the presentation of the contracts (released on the document “ECSC contract presentations guidelines”). During the event, the teams had the chance to present a contract of their choice, earning additional cash rewards.

The final grade varied between:

- Good (extra 60% cash reward of a contract)
- Very good (extra 80% cash reward of a contract)
- Excellent (extra 100% cash reward of a contract)

All the 20 teams presented during the competition with the following grades.

**Table 1: Results of the presentations**

Grade	Number of teams
Excellent	13
Very good	7
Good	0

#### 4.4 PLATFORMS

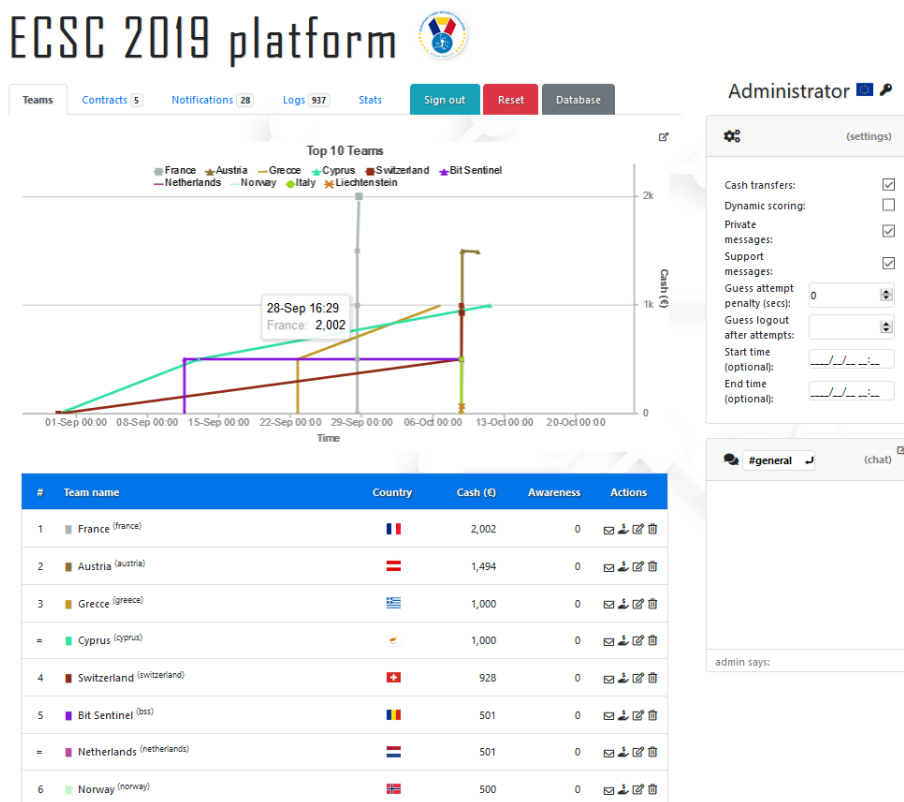
For the planning, testing and execution of the ECSC, ENISA supported the development of the competition by deploying different platforms:

- Test Scoreboard and contracts platform: <https://board.ecsc.eu>
- File Sharing platform (owncloud): Used for information sharing and contingency mechanism: <https://storage.ecsc.eu/>
- ECSC Website: Promotion of the event. Real time scoring information was provided during the challenge to externals interested parties: <https://www.europeancybersecuritychallenge.eu/>

#### 4.5 SCORING PLATFORM (SCORE BOARD)

In order to manage the scores and the contract resolution, ENISA coordinated the improvement of the scoreboard platform created and used last year.

**Figure 1: ECSC 2019 Scoreboard**



The following improvements were collected and implemented for 2019 edition:

- Dynamic Scores
- Improved and detailed boards: Providing detailed information about teams / resolved tasks, which team is working in which contract, etc.
- Improved system logging capabilities: Capture of errors, flags introduced system information, etc.
- Improvements on flag introduction: Flag Types: Static, Regex, Date time, Multiple Choice, File - w/options for case sensitivity
- Reports: Ability to create and get reports (exportable in CSV or other format) that includes different information about the resolution of the contracts
- Chat improvements: Separation between Announcement chats, general chat, team chat
- Option for exporting/access information in real time: Export of the scoreboard in different formats (JSON/XML, etc.), that provides integration with other systems
- Brute force protection
- Time Management: Automatic competition and contracts starting and ending, score freezing at specific time
- Team Management improvement
- Scores management: Penalties, Hints, Attempts, Level Bonuses, Dynamic Scoring, Categories and more
- Dockerization of the platform

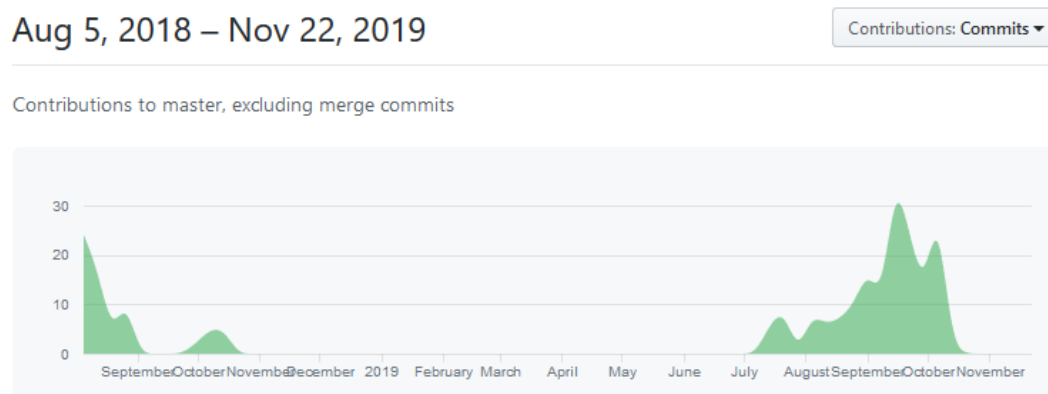
In addition, onsite support by the main developer was provided during the challenge.

The code of the platform is released to the community under EUPL licensing and can be found on Github (<https://github.com/enisaeu/ecsc-gameboard>). For ECSC 2020 it is expected that this platform will be further improved and many changes requested and identified during the challenge will be implemented.

#### 4.5.1 The use of GitHub

In order to improve the coordination of the requested changes, for the first year, GitHub was used as the standard way of requesting changes, notify issues to the main developer and keep track of them.

**Figure 2: Contributions to master**



**Figure 3: Progression of the commits**



Not only ENISA provided feedback: Members of the teams and other collaborators notified bugs and notified issues/bugs and commented the changes.

**Figure 4: Issues and comments**

Filters  Labels 10 Milestones 0 New issue

Clear current search query, filters, and sorts

2 Open ✓ 26 Closed	Author	Labels	Projects	Milestones	Assignee	Sort
Add "Rules" button to link to rules document #32 by peterhuerlimann was closed on Oct 15						1
Use a proper captcha #31 by grzegorz225 was closed on Oct 9						2
The scoreboard should autorefresh #30 by grzegorz225 was closed on Oct 9						
Robustness issues <span style="background-color: #6f42c1; color: white; padding: 2px;">security</span> #25 by floyd-fuh was closed on Oct 7						2
Limiting length of chat/private messages <span style="background-color: #ffc107; padding: 2px;">stabilization</span> #24 by peterhuerlimann was closed on Oct 4						1
Security Issue: Edit Mask of other country <span style="background-color: #6f42c1; color: white; padding: 2px;">security</span> #23 by floyd-fuh was closed on Oct 3						4
Possible Security Issue: reflected callback <span style="background-color: #6f42c1; color: white; padding: 2px;">security</span> #22 by floyd-fuh was closed on Oct 3						2
Un-hide hidden notifications <span style="background-color: #17a2b8; padding: 2px;">enhancement</span> #21 by peterhuerlimann was closed on Oct 3						1
Security issue: Missing PHP secure flag <span style="background-color: #6f42c1; color: white; padding: 2px;">security</span> #20 by floyd-fuh was closed on Oct 3						6
Guess lockout infinite loop <span style="background-color: #6f42c1; color: white; padding: 2px;">security</span> <span style="background-color: #ffc107; padding: 2px;">stabilization</span> #19 by icedevml was closed on Sep 18						4
[SPAM] MySQL credentials are hardcoded <span style="background-color: #17a2b8; padding: 2px;">enhancement</span> <span style="background-color: #6f42c1; color: white; padding: 2px;">security</span> #17 by icedevml was closed on Sep 16						8
Misused Docker container #16 by icedevml was closed on Sep 11						8
Accessing chats and scores on browser tabs #15 by belmontemartin was closed on Oct 15						2

The full track of comments, issues and pull request can be found on GitHub <https://github.com/enisaecsc/ecsc-gameboard/issues?q=is%3Aissue+is%3Aclosed>.



## 4.6 ECSC NEW WEBSITE

The European Cyber Security Challenge website was updated: a new CMS platform was included in order to be able to include new information easily.



The screenshot shows the ECSC 2019 website interface. At the top, there is a navigation bar with links for '2019 CHALLENGE', 'THE HOST', 'PARTNERS', '2019 LEADERBOARD', 'ABOUT', and 'PAST EDITIONS'. The main content area is split into two columns. The left column features a large banner for the 'EUROPEAN CYBER SECURITY CHALLENGE' with the dates '9-11 October 2019' and location 'Bucharest, Romania', along with a 'PARTICIPATE' button. The right column displays the '2019 LEADERBOARD' as of 16:15 on 10 Oct 2019, with a refresh time of 22:30 on 11 Oct 2019. Below the banner is the 'The Organiser' section for Romania, which includes a description of the event and logos for ENISA and the European Commission. To the right of this is the 'Frequently Asked Questions' section, with the first question being 'How can I participate?'. Below the main content, there are two more FAQ items: 'Why should I participate?' and 'Where is the 2019 Challenge hosted?'.

COUNTRY	SCORE
1 Romania	7432
2 Italy	7198
3 Austria	6882
4 Germany	6420
5 Poland	6098
6 United Kingdom	5826
7 France	5484
8 Estonia	4742
9 Spain	4640
10 Portugal	4536

### New ECSC Website

In the ECSC website (<https://ecsc.eu/> or <https://europeancybersecuritychallenge.eu/>) it is possible to find:

- Information about the competition
- Information about the hosting country
- Information about participant countries and national competitions
- Live scoreboard during the event
- Information about past events

## 4.7 COMPETITION CHALLENGES

For ECSC 2019, 38 challenges or “contracts” were provided to participants during the two days of the competition divided into 78 different tasks, these includes activities involving different skills like Crypto, forensics, malware and artefacts analysis, reverse engineering, network forensics, hardware, mobile, steganography, and Capture the flag (CTF) challenges.

The Final list of challenges executed in the event was the following:

**Table 2: Challenges released**

ID	Name	Type
1	binary	reverse, crypto
2	security by design	code review, crypto
3	log analysis	forensics, network
4	incident response	forensics, network
5	cover up	forensics, network
6	unauthenticated encryption	crypto
7	residue number system & crt	crypto
8	ecc	crypto
9	merkle trees	crypto
10	ropper	pwn, reverse
11	oo	pwn, reverse
12	off	pwn, reverse
13	slot	pwn, reverse
14	get-access	reverse, crypto
15	evilmg	web, pentest
16	crack-me	reverse, algorithms, keygen
17	simple-keygen	reverse, keygen
18	debug-service	web
19	baby_heap	pwn, reverse
20	machine-learning	machine-learning
21	younger sister	crypto
22	cryptotime - hash roulette	crypto
23	complicated	forensics, network
24	hack the h4ck3rs	forensics
25	business as usual	pentest
26	evil admin	web
27	protelnet	web
28	random dice	web
29	picasso	forensics, protocol
30	mosaic	stegano
31	plot twist	misc, ransom

32	radios	radio, hardware, crypto
33	elgamal	crypto
34	yellow duck	forensics, misc
35	the bomb	wifi
36	state	web
37	find freddie	escape room
38	blink box	misc, hw

## 4.8 PUBLIC AFFAIRS STRATEGY

The European Cyber Security Challenge (ECSC) Steering Committee decided per ECSC Charter to develop a Public Affairs Strategy for every edition. The main objective of this Public Affairs strategy is to create, distribute and manage a coherent information flow to inform relevant audiences and participating countries about the ECSC final. Moreover, the Strategy provides the input for the Dissemination plan that ensures coherent and synchronised communication.

These documents will contribute to the maturity enhancement of the European Cyber Security Challenge and increase brand exposure. This will draw interested parties from the private sector in context of sponsor opportunities and attract more countries and participants to enrol in future ECSC editions.

The hosting country and ENISA implemented the strategy and the participants were provided with an official media pack, which included the **lines to take**, **brand identity information** and **press releases**. In addition, ENISA provided a **Dissemination Plan** that facilitates timely and coordinated implementation of the strategy amongst all participants and ECSC stakeholders.

This year, also, a [ECSC promotional video](#) from ENISA was released and regular meetings during the competition were scheduled in order to align the media teams from different countries and try to share material and ideas.

### 4.8.1 Women in Cybersecurity in the context of the European Cybersecurity Challenge

With its mission to address the shortage of cybersecurity talent in Europe, the ECSC is also concerned with gender diversity. As a well-established platform, the ECSC is an opportunity to attract more women to the cyber profession. As part of the public affairs campaign of the ECSC, ENISA is investing efforts to attract and identify young women in cyber to join the biggest hacking contest in Europe. The outputs achieved in raising awareness on the urgency to address the talent shortage in cybersecurity before, during and after the competition are the following:

- Before the competition, Deloitte conducted calls with ENISA Public Affairs Team and the Members of the Steering Board to gather their views on the topic and ask them to share national initiatives that aim to bridge the existing gender gap. Deloitte drafted a Whitepaper on women in cybersecurity in the context of the European Cyber Security Challenge.
- During the competition, interviews to young females competing at the ECSC were conducted, and will be published soon.

- After the competition, the **final version** of the whitepaper on women in cyber was leveraged on social media channels of ENISA, published on the ECSC website and through the Deloitte Cyber Team social media powers. In addition, a collage with testimonials and gif animations on young females that participated to short interviews on the topic of women in cyber at the ECSC2019 (in progress). “Working together to change the gender diversity in cybersecurity” or “lifting gender diversity in cybersecurity professions”



Female participants at ECSC2019

The intention in the medium-term is to continue and target these actions under a broader ENISA Women in Cyber initiative. Ultimately, the ECSC can serve as an enabler for achieving a more balanced cybersecurity workforce.

#### 4.9 GALA NIGHT SPEAKER

In a similar way to the way that the independent jury body was selected, a proposal from ENISA to bring a professional speaker to the gala night was launched.








Martina Lindorfer during her presentation

A list with names was proposed and the Steering committee members voted a selection of three preferred candidates. Finally, Martina Lindorfer<sup>3</sup> was selected to perform a motivational speech to the young participants during the awards.

#### 4.10 SOCIAL MEDIA IMPACT

Together with the public affairs strategy a social media report was created, collecting the reactions during the event, according to the report, some of the most remarkable facts regarding to social media impact were the following:

Figure 8: Social media impact

 2113 MENTIONS	 1503 SOCIAL MEDIA MENTIONS	 610 NON-SOCIAL MENTIONS	 1.2 M SOCIAL MEDIA REACH
 22 240 INTERACTIONS	 4654 SHARES	 17 583 LIKES	 657 99% POSITIVE MENTIONS
 6 1% NEGATIVE MENTIONS	 92 MENTIONS FROM BLOGS	 1 MENTIONS FROM FORUMS	 23 NUMBER OF VIDEOS

#### 4.11 CONTINUOUS IMPROVEMENT: IMPROVEMENTS TO THIS YEAR EDITIONS

Following the feedback from previous editions and the requests by the Steering committee representatives, the following improvements were implemented this year:

- No photo policy: Stickers to participants that do not want to be photographed
- Improvements on jury management and independent jury body
- Commcheck prior the competition
- Release of the Who is who document
- Telegram group for internal communication
- Improvement on the problem troubleshooting during the competition
- Improvements to ESCS scoreboard
- Use of Github for pull request, issues and bug reporting
- Alignment of the ECSC in woman in cyber security activities
- Watchdogs, rules and jury enforcement role explained to participants before the competition
- Creation of media meetings during the competition
- Introduction of a speaker for the award dinner/ gala night dinner
- New website with a new look and feel

<sup>3</sup> <https://martina.lindorfer.in/>

# 5. FINAL RESULTS

The final results were the following

**Table 3: ECSC 2019 final results**

Position	Country	Points
1	Romania	8188
2	Italy	7324
3	Austria	7036
4	Germany	6764
5	United Kingdom	6088
6	Poland	6040
7	France	5934
8	Estonia	5502
9	Denmark	5166
10	Portugal	5142
11	Czech Republic	4980
12	Greece	4854
13	Spain	4816
14	Norway	4362
15	Ireland	4206
16	Netherlands	3960
17	Switzerland	3626
18	Cyprus	3384
19	Liechtenstein	2380
20	Luxembourg	2184

## 5.1 POST EVENT ACTIVITIES

As post event activity and, in order to promote the competition and the work that is done at national level, representatives of the winning team of ECSC 2019 were invited by the European Commission to celebrate the 2019 European Cybersecurity Month. CONNECT University organised a special session focused on cybersecurity in practice that provided a great opportunity to get hands-on experience with the latest technology.



Romanian team during Connect University get away day

The representation of the team had the chance to:

- Tour and visit CERT-EU premises in Brussels
- Meet with key cybersecurity stakeholders and other EU officials
- Have a meeting with the responsible for EU-FOSSA project
- Participate in the CONNECT University "Cybersecurity Get Away Day", presenting to young high school students

# 6. LESSONS LEARNT

A lesson-learnt report has been developed by an external observer on behalf of ENISA. It takes into account the feedback provided by ECSC organisers, the ECSC Steering Committee, the Jury, and participants regarding to the following domains:

1. Governance and decision-making aspects
2. Public Affairs: Improvements on the social media communication strategy
3. Challenge: Aspects of the competition to be improved related to the development and setup of the challenge and exercises
4. Logistics: Aspects of the competition related with venue, catering, hotel, transportation, etc.
5. Side Events: Aspects of the competition related with social events and networking meetings
6. Compliance: Aspects of the competition to be improved related with compliance with laws and standards

## 6.1 GOVERNANCE AND DECISION-MAKING ASPECTS

**Table 4:** Lesson learnt on governance and decision-making aspects

Parameter	Observations /Recommendation
<b>Roles and responsibilities</b>	<ul style="list-style-type: none"> <li>• Roles and responsibilities were clearly defined and respected during ECSC planning meetings. The different organisational stakeholders and ECSC Steering Committee members were documented in an ECSC WhosWho which aimed at ensuring transparency about the individual stakeholders and their role in the competition.</li> <li>• Jury members were selected in a clear and transparent manner. The Jury team was established prior to the competition and introduced to the ECSC Steering Committee on the night before the competition so it was clear during the competition who the Jury members were and what their role and responsibilities were. The Jury members applied impartial and objective judgement in their activities.</li> <li>• The Jury members were announced to the participants and were visually identifiable by means of a blue scarf bound around their arms.</li> <li>• Clear "who is who" document, including pictures and role description of ECSC Steering Committee members, Jury members, watchdogs, team coaches, and team captains. The who is who document was disseminated to the participating national teams prior to the competition.</li> <li>• Participants have a decent idea on who to contact in case of questions or technical difficulties during the competition. There was a direct communication line from the participants to the technical staff by means of Signal.</li> <li>• Ad hoc Jury meetings during the second day of the competition prevented the Jury members from monitoring the competition area to spot possible infractions of the ECSC rules.</li> </ul>
<b>Decision-making of the Steering Committee and Jury</b>	<ul style="list-style-type: none"> <li>• ECSC Steering Committee decision-making process efficient and effective during IPC (Brussels) and MPC (Bucharest). Meeting minutes were taken by the Secretariat in order to create an inventory of decisions taken during the planning meetings and an overview of actions to take prior to kick-off of the ECSC main event.</li> <li>• Decision-making in between the Mid Planning Conference and the actual event was on an ad-hoc basis via email, e.g. in relation to the age threshold.</li> <li>• There was an effective and efficient decision-making process between jury members ensured a clear and consistent approach towards incident that</li> </ul>



	<p>occurred during the ECSC finals. All incidents and issues were approached correctly and treated in a timely manner.</p> <ul style="list-style-type: none"> <li>• Technical support staff and platform providers were invited on an ad-hoc basis to the Jury meetings, leading to adequate transparency from a technical perspective allowing the Jury and Steering Committee to make informed decisions with regard to technical aspects of the Challenge.</li> <li>• Team captains and coaches were invited on an ad-hoc basis to the Jury and Steering Committee meetings, leading to adequate transparency about issues and incidents, allowing the Jury and ECSC Steering Committee to take appropriate action and decisions towards award of points for solving a challenge, cheating etc.</li> <li>• Preparatory Steering Committee meetings were held in a constructive manner in preparation of the main competition.</li> </ul>
<b>Transparency</b>	<ul style="list-style-type: none"> <li>• A dedicated communication channel was established for in-game communication between SC and Jury members, for example in relation to changes to the official ECSC2019 agenda, practicalities in relation the event etc.</li> <li>• Questions from participants during the competition, for example, in relation to technical difficulties, were answered in a different way, depending on who gave the answer. When there was a question from one of the participating teams, the answer was not shared through the microphone with all the teams.</li> </ul>
<b>National Participation</b>	<ul style="list-style-type: none"> <li>• The amount of participating countries increased from 17 during ECSC2018 to 20 during ECSC2019. In addition, there were some new countries that attended the ECSC competition as an observer.</li> <li>• Newcomers to the competition were Luxembourg, the Netherlands and Ireland.</li> <li>• Two observing countries were present at ECSC2019, Malta and Finland.</li> </ul>

## 6.2 PUBLIC AFFAIRS

**Table 5:** Lesson learnt on public affairs

Parameter	Recommendation
<b>Monitoring, measurement and analysis (KPIs)</b>	<ul style="list-style-type: none"> <li>• Key Performance Indicators have been defined in the ECSC Public Affairs Strategy in accordance with the Public Affairs goals.</li> <li>• KPIs were monitored and measured by a social media monitoring tool.</li> <li>• ECSC2019 KPIs were analysed and compared with KPIs reported for ECSC2018.</li> <li>• Social media statistics were reported via digital media impact reports to ENISA and the SC on a monthly basis.</li> </ul>
<b>Dissemination Plan</b>	<ul style="list-style-type: none"> <li>• A public affairs dissemination plan was updated as part of the Public Affairs Strategy.</li> <li>• The public affairs dissemination plan was communicated to the individual SC stakeholders and participating teams.</li> <li>• The public affairs dissemination plan was implemented by the majority of the national teams leading to high exposure.</li> </ul>
<b>Key Messages</b>	<ul style="list-style-type: none"> <li>• Key messages were updated compared to ECSC2018 according to the engagement phases as detailed in the dissemination timeline.</li> <li>• The participating teams have successfully adopted the key messages embedded in the ECSC Public Affairs Strategy. An increased level of activity by the national teams has been observed.</li> </ul>

<p><b>Engagement and reach</b></p>	<ul style="list-style-type: none"> <li>• The total reach on social media for the #ECSC2019 campaign from February 1st, 2019 up until October 21st, 2019 is estimated at 1.2 million.</li> <li>• The total amount of mentions on social media for the #ECSC2019 campaign from February 1st, 2019 up until October 21st, 2019 is estimated at 2113.</li> <li>• The total amount of interactions on social media for the #ECSC2019 campaign from February 1st, 2019 up until October 21st, 2019 is estimated at 22 240 (of which 4654 shares and 17 583 likes).</li> <li>• Although the total number of social media reach has decreased as compared to last year, the quality of mentions and amount of interactions has increased.</li> <li>• In order to facilitate a structured and coordinated approach towards public affairs activities, the ENISA Public Affairs Team organised an operational meeting with the Steering Committee, with the support of Deloitte.</li> </ul>
<p><b>Social Media</b></p>	<ul style="list-style-type: none"> <li>• The ECSC Public Affairs Strategy details specific key messages that can be shared across social media networks in order to reach the different target audiences during the different engagement phases as defined in the Strategy. These key messages have been updated compared to the previous version of the ECSC Public Affairs Strategy in order to achieve maximum audience engagement.</li> <li>• Social media platforms were used by ENISA, the members of the ECSC Steering Committee, participating national teams and other relevant ECSC stakeholders prior to, during and after the competition in order to increase awareness about the ECSC.</li> </ul>
<p><b>Website</b></p>	<ul style="list-style-type: none"> <li>• The ECSC website was only updated very shortly before the competition took place.</li> <li>• The official ECSC website (www.ecsc.eu) has been updated prior to the ECSC competition in order to make it more user-friendly, easy to navigate and to strengthen the ECSC branding.</li> <li>• The ECSC website included a real-time feed to the scoreboard, allowing externals to monitor the progress of national teams, leading to transparency in the competition and increased engagement by the target audience, for example, by sharing posts on Twitter on LinkedIn.</li> </ul>
<p><b>Visibility</b></p>	<ul style="list-style-type: none"> <li>• Similar to the previous edition of ECSC, communications about the event were disseminated through relevant channels as detailed in the ECSC Public Affairs Strategy.</li> <li>• There is very limited presence of communications on ECSC on social media platforms used by the participants such as Instagram and Facebook.</li> </ul>

### 6.3 CHALLENGES

**Table 6:** Lesson learnt on challenges

Parameter	Recommendation
<p><b>Design</b></p>	<ul style="list-style-type: none"> <li>• In general, participants were satisfied with the level of difficulty/complexity of the challenges. The challenges included a reasonable learning curve compared to the average level of the participants.</li> <li>• For some challenges, it was not clear to the participants what to submit so it was not possible to solve the challenge.</li> </ul>

	<ul style="list-style-type: none"> <li>• Some challenges only required guessing skills and did not require any hard skills from the participants to solve the challenge.</li> <li>• The majority of the participants was satisfied by the physical security challenge "Free Eddie".</li> <li>• There was not enough diversity in the range of challenges included in the competition, which includes that only a limited set of skills is tested during the competition.</li> <li>• The focus of the challenges was too much on competition instead of collaboration.</li> </ul>
<p><b>Service Providers</b></p>	<ul style="list-style-type: none"> <li>• Service provider was present and supported the participants in technical troubleshooting.</li> <li>• Communication from the service provider to the participants was efficient and effective and supported by instant messaging. In case of emergencies, the technical support staff was available to help participants with troubleshooting.</li> <li>• The service provider has offered a stable and high quality technical network infrastructure to support the challenge.</li> <li>• The service provider communicated transparently and effectively to the Jury and Steering Committee as requested.</li> </ul>
<p><b>Rules</b></p>	<ul style="list-style-type: none"> <li>• Although clearly defined, there was little awareness amongst the participants of the rules.</li> <li>• Rules are ambiguous and unclear to the participants, questions about the rules were not answered in a clear and consistent manner.</li> <li>• Rules about the age limit of the participants was changed between the Main Planning Conference and the competition leading to unclarity up until days before the challenge. The SC has addressed this ad-hoc via email.</li> <li>• No in-game changes were made to the rules. The Jury members ensured a consistent application of all ECSC game rules during the competition.</li> </ul>
<p><b>Enforcement</b></p>	<ul style="list-style-type: none"> <li>• A breach of the rules was approached, treated and followed up by the members of the Jury in a consistent manner. Consequences were agreed upon by the members of the Jury and were communicated in a transparent manner to the SC members and subsequently, to the participants.</li> <li>• Technical capabilities were installed to allow monitoring of infringement of the rules.</li> </ul>
<p><b>Presentations</b></p>	<ul style="list-style-type: none"> <li>• The agenda for the presentations was confirmed and clearly communicated to the SC members and subsequently to the participants.</li> <li>• The five best presentations were presented again during the conference on the third day of ECSC.</li> <li>• The presentations are considered an important aspect of the competition.</li> <li>• The order of the presentations was decided based on the score of the participating teams at the end of the first.</li> <li>• The meeting room in which the presentations took place was right in front of the entrance of the competition venue. As a result, there was a lot of noise and people walking by the presentations. This was distracting to the presenters and the Jury members.</li> <li>• A template for the presentations was provided upfront and respect by the majority of participating teams.</li> </ul>
<p><b>Platform</b></p>	<ul style="list-style-type: none"> <li>• There were access controls preventing participants to start solving challenges before the competition has kicked off.</li> <li>• The ECSC platform as first introduced during ECSC2018 has been successfully deployed in ECSC2019. The overall</li> </ul>

	<p>experience of participants with the platform was positive and in line with their expectations.</p>
<b>Infrastructure</b>	<ul style="list-style-type: none"> <li>• The network infrastructure for the platform was reliable and stable. No major issues or incidents took place with regards to the availability of network infrastructure.</li> <li>• Network capacity and speed was meeting expectations.</li> <li>• There was WiFi available for attendees, organisers and other non-participants in the competition venue. However, it was not able to activate VPN.</li> </ul>
<b>Complexity</b>	<ul style="list-style-type: none"> <li>• In general, participants were satisfied with the level of difficulty/complexity of the challenges. The challenges included a reasonable learning curve compared to the average level of the participants.</li> <li>• Some challenges only required guessing skills and did not require any hard skills from the participants to solve the challenge.</li> </ul>
<b>Scoring</b>	<ul style="list-style-type: none"> <li>• Exceptions on scoring were voted by the Jury.</li> <li>• Scoring of teams was transparent, both internally as externally.</li> <li>• Scoring was not altered during or after the challenge.</li> </ul>

## 6.4 LOGISTICS

**Table 7:** Lesson learnt on logistic

Parameter	Recommendation
<b>Venue</b>	<ul style="list-style-type: none"> <li>• Some of the accommodations (hotels) did not have an easy connection to the ECSC venue.</li> <li>• The competition venue was large enough for all the teams.</li> <li>• The ventilation of the competition area was poor. There was no fresh air so it became very hot after a couple of hours.</li> </ul>
<b>Catering</b>	<ul style="list-style-type: none"> <li>• The quality of the food was poor, especially on the first day. The second day, the organiser has made an effort to offer more qualitative food.</li> <li>• The catering did not indicate the ingredients of the food that was prepared for the participants and the organisers so there was no information on potential allergies.</li> <li>• In the competition venue, there were two restaurants where participants could have lunch.</li> </ul>
<b>In-event communication</b>	<ul style="list-style-type: none"> <li>• Clear in-game communication.</li> <li>• A screen was presented on the wall with an overview of the live scores.</li> <li>• In-event communication between participants and organisers was facilitated by a secure instant-messaging platform.</li> </ul>
<b>Accommodation</b>	<ul style="list-style-type: none"> <li>• The selected accommodations were qualitative and was up to the expectations of the participants.</li> <li>• Some of the accommodations were too far away from the ECSC venue and from the locations where social events were organised.</li> </ul>

## 6.5 SIDE EVENTS

**Table 8:** Lesson learnt on side events

Parameter	Recommendation
<b>Social event</b>	<ul style="list-style-type: none"> <li>The social events did not strengthen the connection between the teams as they were not organised in such a way as to increase the connection between the teams.</li> <li>As participants were allowed to continue working on write-ups and presentations during the evening, some chose not to join the social event, but instead, to focus on the challenge.</li> </ul>
<b>Relevance</b>	<ul style="list-style-type: none"> <li>No conferences or job fairs were organised alongside the competition. However, some of the key sponsors had representatives at the competition venue.</li> </ul>
<b>Format</b>	<ul style="list-style-type: none"> <li>No conferences or job fairs were organised alongside the competition. However, some of the key sponsors had representatives at the competition venue.</li> </ul>
<b>Logistics</b>	<ul style="list-style-type: none"> <li>Access for disabled people was taken into account at the competition venue but was not taken into account during the social events.</li> <li>Social events were organised in locations that were too far away from some of the accommodations (hotels).</li> </ul>

## 6.6 COMPLIANCE

**Table 9:** Lesson learnt on compliance

Parameter	Recommendation
<b>Data protection</b>	<ul style="list-style-type: none"> <li>Stickers were available for participants to indicate they did not want their picture to be taken by photographers, but they were not used in practice.</li> <li>There was no clear communication about how personal data of the participants would be processed by the ECSC organisation.</li> <li>Pictures were taken of people who were wearing no-photo stickers.</li> <li>The WiFi available at the competition venue for participants, organisers and visitors did not allow to set up a VPN connection, therefore, not giving its users a safe environment to do secure/private work during the competition.</li> </ul>

# 7. MATURITY ASSESSMENT RESULTS

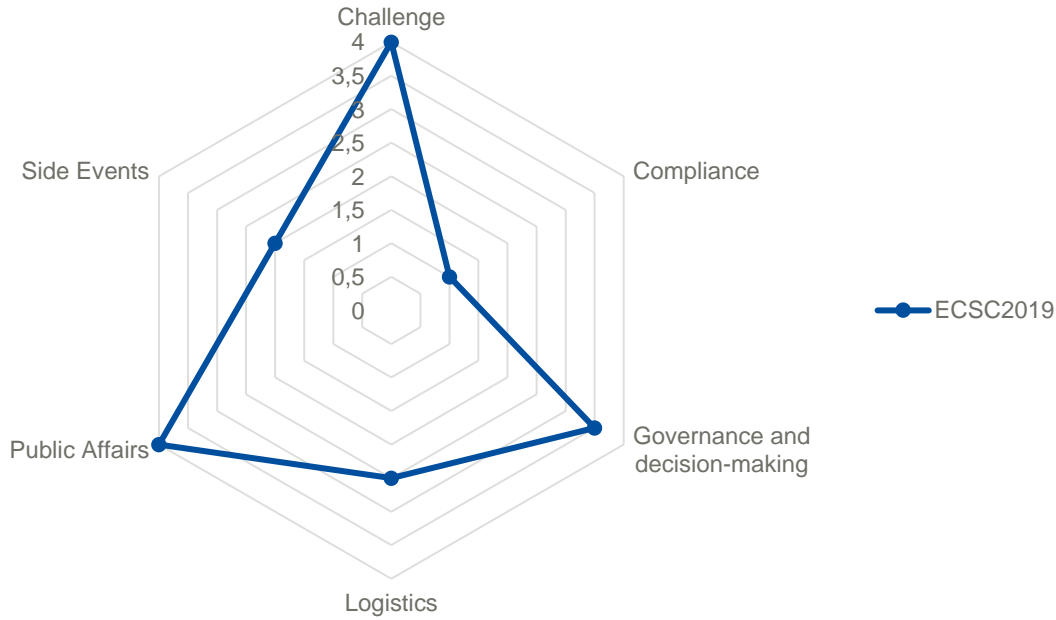
In order to measure the current status of the ECSC project, a maturity assessment, including observations on different areas was developed by an external contractor, these observations have been produced based on the feedback collected from participants, members of the ECSC Jury, members of the ECSC Steering Committee, and attendees to the event. In addition, these remarks reflect the feedback provided by organisers and participants collected by an online evaluation survey, the following domains and parameters were assessed:

**Table 10: Lesson learnt on compliance**

Domain	Parameter
<b>Public Affairs</b>	Monitoring, measurement and analysis (KPIs)
	Dissemination Plan
	Key Messages
	Social Media
	Website
	Visibility
	Engagement and reach
	Complexity
	Design
	Platform
	Presentations
	Rules
	Scoring
	Service Providers
	Enforcement
	Infrastructure
<b>Logistics</b>	In-event communication
	Venue
	Accommodation
	Catering
<b>Side Events</b>	Relevance
	Format
	Logistics
	Social event
<b>Compliance</b>	Data protection
	Transparency
	Roles and responsibilities
	Decision-making
	National Participation
	Decision-making of the Steering Committee and Jury

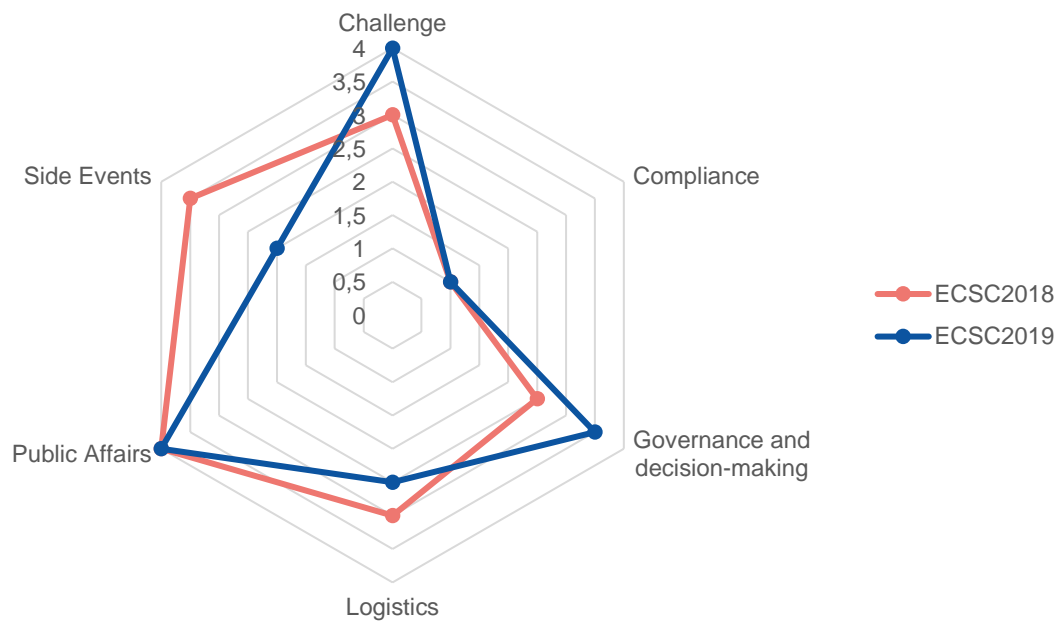
The main results on the report are summarised below:

**Figure 9: Maturity Assessment results**



Compared to the ECSC2018 edition, the results are the following:

**Figure 5 Process maturity per year**



## 8. ECSC 2020

The final of the 2020 edition of the European Cyber Security Challenge will take place at Vienna in November 2020 where, at least, 22 countries are expected to participate. The latest updates will be published on ECSC 2020 website: <https://www.europeancybersecuritychallenge.eu/>



European Cyber Security Challenge 2020 logo





## 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](http://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](http://enisa.europa.eu)

