Tackling the Gender Gap in Cybersecurity Education

Gabriele Costa
IMT School for Advanced Studies
Lucca, Italy
gabriele.costa@imtlucca.it

Silvia De Francisci
IMT School for Advanced Studies
Lucca, Italy
silvia.defrancisci@imtlucca.it

Margherita Renieri
IMT School for Advanced Studies
Lucca, Italy
margherita.renieri@imtlucca.it

Serenella Valiani
IMT School for Advanced Studies
Lucca, Italy
serenella.valiani@imtlucca.it

Abstract

The gender gap in cybersecurity remains a persistent and concerning issue. Despite efforts to promote diversity and inclusivity, women remain significantly underrepresented in cybersecurity roles. One of the primary factors contributing to the gender gap in cybersecurity is the lack of female representation and encouragement in STEM (Science, Technology, Engineering, and Mathematics) fields. Stereotypes and societal biases often dissuade girls and young women from pursuing careers in these fields, leading to a smaller pool of women candidates entering the cybersecurity workforce.

In this work, we present *CyberTrials*, a CTF-based cybersecurity program for Italian upper secondary schoolgirls. Our program utilizes a *gamified hybrid learning* environment, combining theoretical online lectures with interactive team activities in the form of competitive games. Although each team autonomously tackles the game challenges, participants may adopt prosocial behavior, including collaborative peer interactions and mentoring. This collaborative approach enhances problem-solving skills and fosters a culture of mutual support. Here, we outline the technical details of our approach, including the technologies involved and the data collected during CyberTrials. Our analysis, comprising both quantitative and qualitative findings and demonstrates three key outcomes: (*i*) the successful engagement of participants; (*ii*) the facilitation of the learning process through the introduction of entry-level CTF challenges, and; (*iii*) a remarkable shift in participants inclination towards pursuing STEM studies at the university.

CCS Concepts

• **Social and professional topics** → **Women**; **K-12 education**; • **Security and privacy**;

Keywords

Capture the Flag, gender gap, cybersecurity, upper secondary school, hands-on training

SIGCSE TS 2025, February 26-March 1, 2025, Pittsburgh, PA, USA

ACM ISBN 979-8-4007-0531-1/25/02
https://doi.org/10.1145/3641554.3701807

ACM Reference Format:
Gabriele Costa, Silvia De Francisci, Margherita Renieri, and Serenella Valiani. 2025. Tackling the Gender Gap in Cybersecurity Education. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE TS 2025), February 26-March 1, 2025, Pittsburgh, PA, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3641554.3701807

1 Introduction

The gender gap in cybersecurity is a pressing issue that demands attention and actions [49].[1] This gap deprives the industry of valuable perspectives [6, 32] and poses significant challenges to effectively addressing the growing threat landscape. To comprehend and address this gap, it is crucial to recognize that it is deeply interconnected with the broader gender disparities within all the STEM fields [3, 47], which becomes dramatically clear in universities. For instance, during the academic year 2022/2023, 56.5% of new students enrolled by Italian universities were women. However, only 20.8% of these students chose a STEM course (men 40.3%) [35]. Achieving gender balance in STEM fields in universities requires promoting these disciplines and getting rid of bias and stereotypes starting from upper secondary school [8, 28]. There, girls often face societal expectations [42] and cultural conventions [33] that discourage their engagement with STEM subjects. By implementing initiatives that promote inclusiveness and break down gender stereotypes, researchers in CS education are exploring and understanding how to better integrate women and encourage more girls to pursue STEM subjects [8, 28]. These initiatives apply many different approaches, including mentoring programs [44], outreach efforts to encourage girls to pursue STEM [41, 45], and courses or internships designed exclusively for women [5]. All these programs offer girls access to first-hand experiences through introductory yet engaging activities. Unfortunately, implementing the same approach in cybersecurity is extremely challenging, due to the highly technical nature of even the most basic activities.

In this paper, we present the results obtained through *CyberTrials*, a national entry-level, game-based training program in cybersecurity for upper secondary school girls. The objective of CyberTrials aligns with the guidelines of the Measure #65 of the Implementation Plan for the National Cybersecurity Strategy 2022-2026.[2] The program provides female students with an initial training cycle focused on the foundations of cybersecurity. Hence, students have the opportunity to (*i*) develop their digital skills, (*ii*) shape their digital

[1] E.g., in 2022 women only held 25% of cybersecurity jobs globally [39].
[2] https://www.acn.gov.it/ACN_Implementazione.pdf (in Italian).

citizen profile, and (*iii*) enhance their technical knowledge and understanding. CyberTrials combines traditional lectures with hands-on activities based on *Capture-The-Flag* (CTF) [14], to improve learning efficiency and consolidate participants' understanding. We designed hands-on activities by incorporating game elements (e.g., scoreboards and badges) into non-game contexts. This approach, known as *Gamification* [36], both (*i*) enhances engagement and motivation and (*ii*) facilitates the retention of knowledge [7, 15]. Our findings suggest that CyberTrials achieves these goals as it (*i*) successfully engages students, (*ii*) favors the learning process, and (*iii*) remarkably increases participants' inclination towards pursuing STEM studies. These results are obtained by immersing students in technical operations such as network scanning, web vulnerability detection and exploitation, cryptography, and steganography. Noticeably, most of these subjects are also addressed during the European Cyber Security Challenge (ECSC).[3]

The paper is structured as follows. In Section 2, we provide some background information and related works. Section 3 presents a comprehensive overview of participants' educational context. Section 4 details the CyberTrials program, its scope, and objectives. Section 5 describes the design and implementation details of the CyberTrials infrastructure. Section 6 discusses the achieved results and data collected during the program. Section 7 draws the conclusions and sketches some future research directions.

2 Related Work and Background

Recently, there was a growing interest in cybersecurity, including education and training [25]. Effectively teaching cybersecurity is highly challenging and advanced training methodologies are required. Among them, CTFs (e.g., see [29, 34]) and gamification approaches (e.g., see [30]) are often used to enhance engagement.

CTFs prompt participants with interactive challenges that emulate real-world scenarios and stimulate practical skills and competitiveness. CTF challenges cover various areas such as cryptography, reverse engineering, web security, binary exploitation, and forensics [27]. Upon successful completion of a challenge, participants obtain a *flag*, i.e., a textual code testifying the resolution. Players receive points for each flag they submit, and whoever has the highest score wins the competition. Following [46], CTF competitions come in two primary forms: jeopardy and attack-defense (AD). In a jeopardy-style CTF, each challenge is a stand-alone exercise, and the flag score is either fixed or dynamic, e.g., decreasing after each solution. Variants like *quest* CTFs incorporate storytelling and progressive challenges. Conversely, in an AD CTF, each team manages a vulnerable system, getting points by attacking opponents' systems while defending their own. Unlike CyberTrials, the other girl-only CTFs we are aware of, are standalone events [20, 26, 38], not integrated with an educational program. These events are almost inaccessible to girls who lack prior skills.

Gamification is the integration of game elements into non-gaming contexts like classrooms and online courses [1, 16]. By harnessing the principles of game design, educators can create immersive learning environments that encourage students to actively participate, set and achieve goals, and gain a deeper understanding of the subject matter [19]. For instance, the Girls Cybersecurity Camp [12] integrates a cybersecurity-based escape room in an educational summer camp with 48 participants. The project is similar to ours in terms of purpose and techniques. Their results outline positive effects on the overall interest of the participants in STEM subjects.

Although potentially effective, programs like [12] do not scale on large numbers of participants and, thus, cannot assess the gender gap society-wide. As described in Section 4, CyberTrials relies on gaming and training facilities that were specifically designed to support hundreds of participants from all over the country.

Beyond cybersecurity, several initiatives have been proposed to tackle the gender gap in STEM disciplines, in general, and CS, in particular. For instance, Basiglio et al. [2] evaluate the influence of Coding Girls [43], a CS-oriented training program on girls' educational decisions. Burge et al. [4] report a CS summer camp for high school girls with the same objectives. Although both programs report positive impact on programming skills and confidence, there is no significant effect on students' aspirations to pursue STEM studies. This outcome might derive from insufficient engagement with the subject matter, which gamification can foster. For instance, Gutica [17] presents a four-day workshop with 25 girls that integrates an educational video game to teach programming via block coding, with positive outcomes in terms of interest in STEM fields. Unlike ours, the programs discussed above do not relate to cybersecurity and they are meant to target a small audience.

3 Reference Educational Context

CyberTrials targets students who attend *upper secondary school* (aged 14 to 19). Italian upper secondary education has specialized pathways for students with academic or work aspirations, comprising lycea, technical institutes, and vocational institutes in line with the European Qualifications Framework (EQF).[4] These curricula include shared subjects from Italian language and literature to mathematics, from foreign languages to physics and chemistry. All schools share a common set of subjects and learning objectives. Then, lycea have curricula focused on, e.g., humanities, sciences, arts, and foreign languages. Technical institutes, categorized into economic and technological, focus on foundational and practical skills with some attention to professionalizing students. Vocational institutes offer personalized learning pathways and practical training plans to prepare students for specific employment sectors organized in eleven study fields. Vocational institutes specifically aim to equip students with practical skills. In the 2023/2024 academic year, there were 2,631,879 students enrolled in upper secondary school, with 51.4% attending lycea, 31.7% attending technical institutes, and 16.9% attending vocational institutes [40]. All students' activities are recorded in the Educational, Cultural, and Professional Profile (PECUP) [22], akin to their curriculum. This includes the "Percorsi per le Competenze Trasversali e l'Orientamento" (PCTO)[5] a dynamic method of education applied to the last three years of upper secondary school. PCTO pathways should take place in a real or simulated professional or academic environment, and value students' learning methodologies, possibly allowing for the development of cross-disciplinary skills. Each upper secondary school

[3] https://ecsc.eu/

[4] https://europa.eu/europass/en/europass-digital-tools/european-qualifications-framework

[5] Defined through law No. 145/2018.

Table 1: List of CyberTrials modules.

M.	Topics	Challenges
0	Introduction	Usage of Discord and CTFd
1	Team building	Teamwork, strategy
2	Ethics and Laws	Censorship, cookie policy, crime reconnaissance
3	Linux and shell	SSH, file management utilities
4	Network	Usage of wireshark, netcat, nmap, FTP service
5	Web	HTTP request-response, developer tools, RCE
6	OSInt	Web archive, search engines, exiftool
7	Cryptography	Usage of cipher, steganography, base32
8	Social engineering	Phishing and spoofing

allocates a different amount of hours for PCTO in line with the objectives of its study program. Hence, technical and vocational institutes have more PCTO hours than lycea. Students are certificated by their school after completing the PCTO activity. The PCTO hours are then deducted from the total hours of their school program. Finally, PCTO activities are discussed during the final high school exam to obtain the diploma.

4 CyberTrials Program

Here we present the technical aspects behind the third edition of CyberTrials carried out remotely from January 22nd, 2024 to March 18th, 2024.[6]

4.1 Program Structure and Objectives

The main goal of the training program is to introduce the participants, who had no prior skills, to basic competencies and a general understanding of some aspects of cybersecurity, while addressing social biases and encouraging their pursuit of STEM fields in university. The entire program, including the final, in-person event, was free and the enrollment was open to all upper secondary school students identifying as women. This initiative is inspired by the findings outlined in [25], which explores cybersecurity perceptions among high school girls. The study highlights effective strategies for engaging adolescent girls in cybersecurity, such as creating girls-only environments, encouraging collaborative learning, providing role models, and involving them in practical and creative activities.

Weekly online lectures[7] were proposed to introduce the program's topics to the participants (see Table 1). Each lecture was presented by one or more speakers from either industry (45.5%) or academia (54.5%). The program was also carefully designed to ensure gender balance among the speakers. In particular, 7 out of 11 (63.6%) were women. The topics were presented assuming no prior knowledge. Thus, the program first introduced the CTF context, soft skills and ethical aspects of cybersecurity (M0 – M2) and then addressed hard skills including, e.g., shell scripting (M3), network security (M4) and cryptography (M7). Moreover, the program included two seminars during the final two weeks: one on the empowerment of women in STEM fields, and one on how to approach a live CTF contest.

Theoretical topics were complemented with practical, hands-on training consisting of two CTFs jeopardy. We chose jeopardy-style because it is the best suited for a non-professional audience [46]. All the challenges were developed and tested by a technical team of computer scientists, which also ensured gender representation (75% women). This was meant to avoid potential gender biases even in the innermost, technical details of each challenge. The two CTFs were continuously played during the entire training program. One CTF was a *team-oriented* (TCTF) while the other was individual (ICTF). The ICTF had two primary goals, i.e., (i) hosting training challenges (e.g., taken from past editions) and (ii) monitoring the active participation of enrolled students. In particular, after each lesson, four challenges were released concerning the lesson's topic, as listed in Table 1. Out of them, three challenges were published on TCTF. The three challenges were ordered by complexity from the easiest (score range from 10 to 40) to the hardest (score range from 70 to 120). Also, solving the first (second) challenge was mandatory to unlock the second (third). Finally, each challenge was provided with at least one *hint*, which participants could acquire by paying a few points (e.g., 5). The fourth challenge was, instead, released on ICTF. ICTF challenges were of minimum complexity and had no score as their goal was to check the active participation necessary to assign the students with the PCTO certificate. In particular, participants were obliged to complete each challenge before the next lecture. Failure to solve a challenge on time resulted in a warning, with two warnings leading to exclusion from the program. After exclusions, a team merging process was carried out to ensure fairness. Participants who completed the CyberTrials program received a PCTO certificate for 46 to 50 hours (depending on their participation in the final event).

4.2 Quest CTF

TCTF was a *gamified quest* CTF. Its gamification elements are competition with a final prize, incremental difficulty, and a role-playing setting. The competition ended with the top 20 teams on the scoreboard being admitted to the final event. The final in-person competition took place on June 8th determining the overall winners. The final was a 6-hour jeopardy CTF with 13 challenges.[8] The story follows a criminal group launching ransomware attacks, and participants (impersonating a task force) have to block the attacks and uncover their authors. Initially, an insider emerges to help the participants, but in the end, she turns out to be the leader of the ransomware group, trying to act as a decoy. Challenges were integrated with the story through descriptions, hints and attachments.

Figure 1 shows the four challenges released for module 3 (M3), about Linux and shell. The ICTF (leftmost) challenge just asks participants to establish an ssh connection to a remote machine and it is unrelated to the quest. The three TCTF challenges (right), instead, include references to the story. In particular, in "Knocking on heaven's backdoor" (20 points) participants must find a way to interact with a remote ssh terminal used for an attack on CyberBank, presented in the previous module (M2). Briefly, the ssh server was configured to return a constant string and immediately drop the connection. The string that at first sight looked like garbage text was, in fact, the flag in ASCII art format. In "Trees of Threes" (40 points), participants were asked to find and read a file via ssh. Finding the right file among many candidates required filtering

[6]The second edition was reported in [13].

[7]The lectures were recorded, allowing participants to either follow them live or catch up in the following days.

[8]The last 13 challenges concluded the quest story.

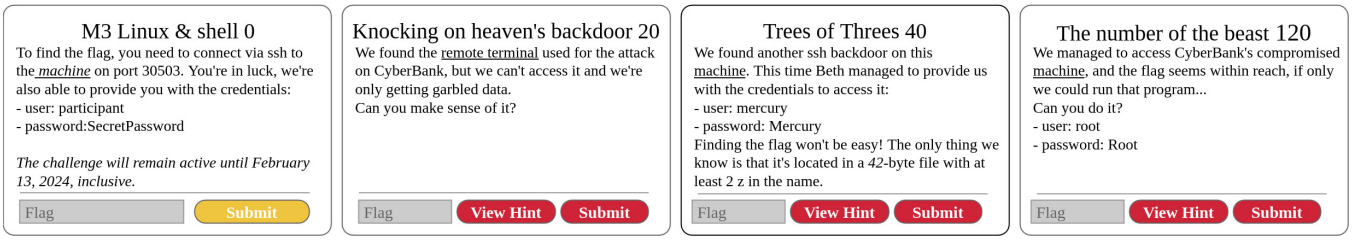

Figure 1: The challenge of ICTF (left), and the three challenges of TCTF (right) of the 3rd module about Linux and shell.

them by some features such as dimension, creation data, permissions and ownership. Again, the challenge description refers to the story, i.e., to the character called Beth. Finally, the challenge "The number of the beast" (120 points) was about privilege escalation to gain execution permissions over a file. This was achievable through a misconfigured utility running in background. Again, this challenge has to do with CyberBank. Once the three challenges were completed, teams discovered the name of the ransomware group.

4.3 Learning Models

A goal of CyberTrials is promoting prosocial behavior among participants. Students should actively collaborate and support each other within their teams and across the program, creating a sense of community and shared responsibility. Hence, participants were engaged in Reciprocal Peer Tutoring (RPT) [9] involving role-switching among individuals at the same educational level. RPT promotes individual responsibility, accountability, and group solidarity by enabling students to both learn and contribute to their peers' learning experiences, thereby reducing power differentials and fostering mutual growth. This outcome highlights how prosocial behaviors and citizenship values are integrated into the competitive nature of activities, fostering a sense of community and shared goals. From the level of communication, students enhance their communication, teaching, problem-solving, and collaborative skills, leading to a deeper understanding of knowledge and improved academic achievement. The RPT environment has been implemented through the communication channels presented in Section 5.

5 Infrastructure and Tools

One of the distinguishing features of CyberTrials is its tool suite. Indeed, CyberTrials has two peculiar requirements for accessibility and engagement that tools must satisfy. The accessibility requirement is to allow participation even to students not provided with a personal computer, e.g., using a tablet or mobile.[9] The engagement requirement is to foster collaboration and mutual support between geographically sparse participants.

The overall architecture of the CyberTrials platform is illustrated in Figure 2. Students have a double role, i.e., they are both individual participants and team members. Participants join the program by registering to the ICTF platform (leftmost, yellow box). Thus, each participant also gets access to (*i*) the official Discord [11] server and (*ii*) the Zoom [48] channel for the lessons. Then, a custom Discord Bot automatically assigns each participant to a random,

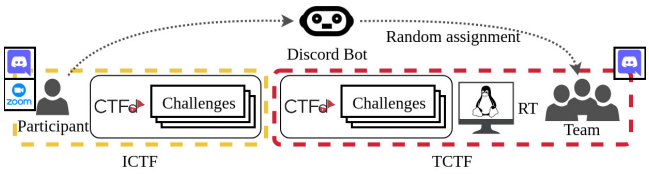

Figure 2: CyberTrials CTF platform.

four-member team, granting them access to the TCTF platform (rightmost, red box). Both the CTF platforms consist of a customized installation of CTFd [10] hosting the challenges as described in Section 4.1. Furthermore, TCTF hosts remote terminals (RT) for each team running on Webtop [31] Docker [21] containers. These remote terminals are accessible via web browser and are pre-configured with all the security tools needed during the competition. Both the CTFd instances and the Webtop containers were deployed on a private cloud platform.[10] Each Webtop terminal had 2 dedicated CPUs, 2 GB virtual RAM and 2 GB virtual hard disk. The system could spawn up to 100 Webtop terminals in parallel. Also, the Webtop management system is provided with a waiting queue (in case more than 100 requests are received) and a garbage collector suspending inactive terminals.

The platform is designed to fulfill our initial requirements. In terms of accessibility, Webtop terminals ensure that challenges can be solved using mobile devices. Discord serves as the main communication channel, with private channels for team coordination and public channels for official announcements, training material, support, and thematic discussions. Live Zoom lectures were recorded and shared through Discord, thus allowing asynchronous access. In terms of engagement, the random team formation mechanism forced the participants to meet other students and establish collaborations to achieve a common goal. Also, the private Discord channels provided a synergic workspace where teams could chat and make voice calls. All in all, the platform is meant to host a *peer education* environment [18]. *Transfer-of-knowledge sequences* were obtained through the training material and official support channels where participants could receive technical help from the organizing team. Finally, *collaborative sequences* were provided via the open discussion channels where participants helped each other and naturally assumed expert and learner roles, depending on their knowledge and skills.

[9]Notice that similar cybersecurity [20, 26, 38] and CS [2, 12] programs require laptops.

[10]Implemented with two dedicated VMWare ESXi machines, each equipped with 128 Intel® Xeon® Gold 5218 CPUs @ 2.30GHz and 2 TB hard disks.

Table 2: Number of participants enrolled and finalists.

Participants	#	Origin (%/Norm)					School year (%)					School pathways (%)						
		NW	NE	C	S	I	1st	2nd	3rd	4th	5th	IT	E	AS	H	HS	L	oth.
Enrolled	779	15/0.56	11/0.56	19/0.95	40/1.75	15/1.38	6	8	39	29	18	43	11	26	4	3	3	10
Finalists	68	24/0.89	13/0.67	13/0.65	32/1.39	18/1.63	3	9	23	40	25	60	1	26	4	3	0	6

6 Evidence and Perception

This section presents the most relevant outcomes and impact of the CyberTrials program. We recall that our goal is to evaluate the training program. Hence, we do not report data from the final event, as they only refer to a limited subset of the enrolled students.

6.1 Description of the Participants

Overall, 779 girls enrolled to CyberTrials and 68 girls have been admitted to the final. Table 2 summarizes the geographical origin, year and type of school for all the enrolled students and for the finalists only. Geographical origins[11] are normalized based on the distribution of the overall female population [24]. For instance, 15% of the enrolled students were from the northwest (NW), where 26.8% of the national female population resides, thus leading to a normalized value of $15/26.8 \simeq 0.56$.

Some facts emerge from the data in Table 2. The enrollment was above the average in regions S and I, while NW and NE were under-represented. Among the finalists, however, the distribution slightly changed, highlighting that students from NW, NE and I performed better. In terms of age, most enrolled students attended the third or fourth year of upper secondary school. This is expected since (i) students in the first two years cannot receive PCTO, and (ii) fifth-year students are focused on their final upper secondary school exams (see Section 3). Among the finalists, there is a noticeable shift toward the last two years, likely due to improved skills and prior participation in similar courses or past editions of CyberTrials. Most students are from STEM-oriented institutes, namely IT Technical Institutes (IT), Economic Technical Institutes (E), and Applied Scientific Lyceums (AS). This is even amplified among finalists, rising from 79% to 88%. Again, this is expected as these institutes have curricula in CS [37]. Noticeably, although none of the students from the Language Lyceum (L) made it to the final event, the ratio of students from Human Lyceum (H) and Human Science Lyceum (HS) did not change. This might suggest that the competition is also accessible to students with no formal CS education.

6.2 Self Assessment

The participants (treatment group) and a control group completed one questionnaire before the start of the program and another after the last lecture.[12] The control group consisted of students from the same school context, matched in age with the treatment group but not enrolled in CyberTrials. By comparing the outcomes of the two groups, we determine whether the observed changes in the treatment group are attributable to the treatment itself or to external factors. The treatment group consisted of 245 participants who attentively[13] filled out the two questionnaires. The control group counted 45 questionnaires (out of 52 respondents).

Table 3: Self-assessed satisfaction questions.

Statement	TD	D	A	TA
Lectures were interesting	1.2%	8.2%	63.3%	27.3%
Lectures were difficult	2.0%	18.8%	53.9%	25.3%
Challenges were interesting	0.4%	4.9%	52.7%	42.0%
Challenges were difficult	0.8%	6.9%	44.1%	48.2%
Importance of team-working	7.4%	16.7%	36.3%	39.6%

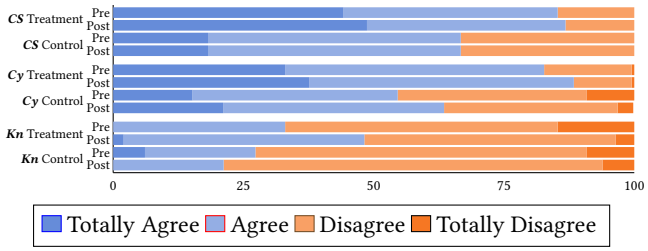

Figure 3: Interest in computer science (*CS*), interest in cybersecurity (*Cy*) and knowledge in cybersecurity (*Kn*).

The second questionnaire's satisfaction-measuring questions and answers are listed in Table 3. Both lectures and challenges were considered interesting (91% and 95%, respectively) and difficult (79% and 92%, respectively), while 76% consider teamwork crucial. Noticeably, the majority (65%) considered the proposed challenges fair. These results confirm that the demanded effort was adequate w.r.t. the initial skills.

Figure 3 shows the results of self-assessment questions for the two groups. Answers were ranked between totally agree and totally disagree. Interestingly, the treatment group exhibits a growing trend in all three cases. Instead, the control group shows mixed results. For *CS*, they remain stable, while for *Kn* they even show a negative trend. This confirms the effectiveness of CyberTrials in providing cybersecurity knowledge. Although less evident, a similar argument applies to the interest toward *CS*.

Among the participants who completed both questionnaires, 184 declared interest for the university. Figure 5 shows the interest in pursuing STEM they report in pre- and post-questionnaires. The answers show a remarkable shift in the interest in STEM[14],

[11] Areas are defined by the Italian Institute of Statistics [23]: northwest (NW), northeast (NE), center (C), south (S), and islands (I).

[12] The questionnaires were approved by the Joint Ethics Committee of Scuola Normale of Pisa, Scuola Sant'Anna of Pisa, and IMT School for Advanced Studies on 16/01/23, by the resolution n.4/2023. Questionnaires were administered online in Italian, questions are available at https://docs.google.com/document/d/1Srh2S4X6O3zXo7d_GP0zQZG9In3a9bzoRxFvLH6u0VQ/edit?usp=sharing.

[13] An attention check question was included for this purpose.

[14] Noticeably, nobody initially declaring interest in STEM swapped to no STEM.

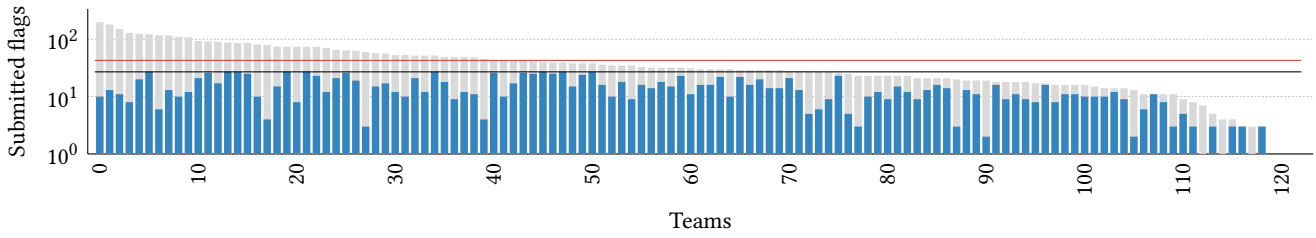

Figure 4: Number of flags submitted by each team.

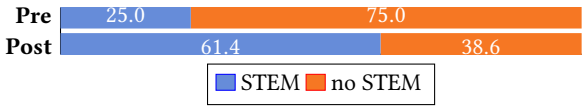

Figure 5: Interest (in %) in pursuing STEM fields.

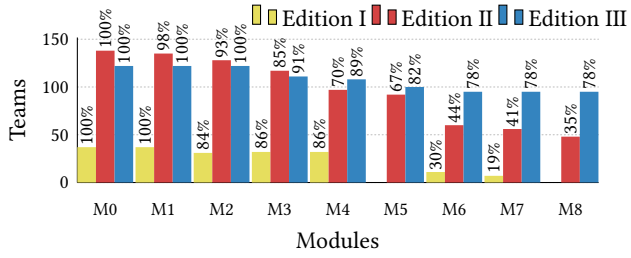

Figure 6: Teams attendance during the three editions.

outlining that CyberTrials (and CTF in general) may consolidate confidence in one's skills through active learning.

Finally, participants provided suggestions and comments on the program. For instance, one participant commented *"Interesting and well-managed lessons. I found the topics covered very engaging. I would have preferred more individual challenges. Thanks for the experience!"* These comments are valuable for improving the program and will be carefully evaluated before the next edition.

6.3 Teams Activity

In this section, we present data about the activity of the teams. Initially, 122 teams took part in CyberTrials. Then, 27 teams were merged, and 1 was disbanded (see Section 4.1). Figure 6 compares the number (and percentage) of teams that submitted at least one flag (either correct or wrong) to the first challenge of each module, along the three editions.

Beyond the difference in terms of the absolute number of teams, the figure shows a positive trend in the teams' dropout rate. In particular, the first year's participation was quite stable until the fifth week (M4), i.e., the last module with challenges that accounted for the selection of the finalists. Then, module M5 was skipped, and the number of participants dropped significantly to 19% during the last module (M7). In the second edition, the dropout rate was more uniform, with the highest decrease between M5 and M6 (−23%), with the final percentage of teams of 35%. This highlights the positive role of the competition. The same trend was confirmed this year, with even better numbers (closing at 78%). The improvement could be the result of the introduction of ICTF.

Figure 4 shows the number of flags, both correct (blue bar) and wrong (grey bar) submitted by all the 122 teams. The maximum number of correct flags was bound to the number of challenges, i.e., 27 (horizontal, black line). The 10 most active teams submitted more than 100 flags, the average number of submissions per team was 43 (red line) and the total number of submitted flags was 5220. The overall number of correct submissions was 1615, with an average of 13.24 per team. Among all the teams, 9 completed all 27 challenges correctly but only 7 of them used no hints. Compared to the previous edition, we have made adjustments to enhance the difficulty of the challenges. These numbers confirm that the overall level of complexity was adequate w.r.t. skills of the participants.

7 Conclusion

In this paper, we presented the third edition of CyberTrials, a cybersecurity program tailored for upper secondary school girls. Its distinguished feature is a unique gamified, hybrid learning infrastructure. Evidence shows significant enhancement in both engagement and education in cybersecurity. These results were achieved through a systematic evaluation of the provided contents and the implementation of a gaming experience revolving around a quest CTF competition. The main outcome was a remarkable increase in participants' interest in pursuing STEM studies at the university level. These results underscore the key role of initiatives like CyberTrials in addressing the gender gap in cybersecurity and, more broadly, in CS. Our program also aims to enhance the reproducibility and accessibility of this approach. This includes ensuring that the required skills and tools are attainable and user-friendly, serving as a model for similar initiatives.

Our approach may be extended in several directions. For instance, a line of investigation would systematically measuring the influence of prosocial behaviors and the advantages of cooperative learning fostered among participants. Another important area for research would be including personalized materials, tools, and support resources for students with special educational needs. For instance, specific support may be developed for students having a cognitive disability, who amount to approximately 2% of Italian students enrolled in upper secondary school.

Acknowledgments

This work was partially supported by project SERICS (PE00000014) under the NRRP MUR program funded by the EU - NGEU.

References

[1] Alessandra Antonaci, Roland Klemke, Christian M Stracke, Marcus Specht, Mario Spatafora, and Kamelia Stefanova. 2017. Gamification to empower information security education. In *International gamiFIN conference 2017*. 32–38.

[2] Stefania Basiglio, Daniela Del Boca, and Chiara Pronzato. 2023. The Impact of the "Coding Girls" Program on High School Students' Educational Choices. *CESifo Working Paper* 10235 (2023), 18.

[3] David N Beede, Tiffany A Julian, David Langdon, George McKittrick, Beethika Khan, and Mark E Doms. 2011. Women in STEM: A gender gap to innovation. *Economics and Statistics Administration Issue Brief* 04-11 (2011), 11.

[4] Janet E. Burge, Gerald C. Gannod, Maureen Doyle, and Karen C. Davis. 2013. Girls on the go: a CS summer camp to attract and inspire female high school students. In *Proceeding of the 44th ACM Technical Symposium on Computer Science Education* (Denver, Colorado, USA) *(SIGCSE '13)*. Association for Computing Machinery, New York, NY, USA, 615–620. https://doi.org/10.1145/2445196.2445376

[5] Jill M Bystydzienski, Margaret Eisenhart, and Monica Bruning. 2015. High school is not too late: Developing girls' interest and engagement in engineering careers. *The Career Development Quarterly* 63, 1 (2015), 88–95.

[6] Lindy Cameron and Jonathon Gill. 2021. *Decrypting Diversity – Diversity and Inclusion in Cyber Security*. Technical Report. National Cyber Security Centre. https://www.ncsc.gov.uk/files/KPMG-and-the-NCSC-Decrypting-Diversity-2021-report.pdf

[7] Ilaria Caponetto, Jeffrey Earp, and Michela Ott. 2014. Gamification and education: A literature review. In *European Conference on Games Based Learning*, Vol. 1. Academic Conferences International Limited, United Kingdom, 50.

[8] David Card and A Abigail Payne. 2021. High school choices and the gender gap in STEM. *Economic Inquiry* 59, 1 (2021), 9–28.

[9] Yi-Chia Cheng and Heng-Yu Ku. 2009. An investigation of the effects of reciprocal peer tutoring. *Computers in Human behavior* 25, 1 (2009), 40–49.

[10] Kevin Chung. 2017. CTFd. https://ctfd.io

[11] Jason Citron. 2015. Discord. https://discord.com/

[12] Cariana J Cornel, Dale C Rowe, and Caralea M Cornel. 2017. Starships and cybersecurity: Teaching security concepts through immersive gaming experiences. In *Proceedings of the 18th Annual Conference on Information Technology Education*. Association for Computing Machinery, New York, NY, USA, 27–32.

[13] Gabriele Costa, Silvia De Francisci, Serenella Valiani, and Paolo Prinetto. 2023. Why Mary Can Hack: Effectively Introducing High School Girls to Cybersecurity. In *Proceedings of the 18th International Conference on Availability, Reliability and Security (ARES '23)*. Association for Computing Machinery, New York, NY, USA, Article 71, 8 pages. https://doi.org/10.1145/3600160.3605009

[14] CTFtime. 2012-2024. What Is Capture The Flag?,. https://ctftime.org/ctf-wtf/

[15] Darina Dicheva, Christo Dichev, Gennady Agre, and Galia Angelova. 2015. Gamification in education: A systematic mapping study. *Journal of educational technology & society* 18, 3 (2015), 75–88.

[16] Eyvind Garder B Gjertsen, Erlend Andreas Gjære, Maria Bartnes, and Waldo Rocha Flores. 2017. Gamification of Information Security Awareness and Training.. In *ICISSP*. 59–70.

[17] Mirela Gutica. 2021. Fostering High School Girls' Interest and Attainment in Computer Science. In *Proceedings of the 26th ACM Conference on Innovation and Technology in Computer Science Education V. 1* (Virtual Event, Germany) *(ITiCSE '21)*. Association for Computing Machinery, New York, NY, USA, 471–477. https://doi.org/10.1145/3430665.3456353

[18] Cynthia R Haller, Victoria J Gallagher, Tracey L Weldon, and Richard M Felder. 2000. Dynamics of peer education in cooperative learning workgroups. *Journal of engineering education* 89, 3 (2000), 285–293.

[19] Juho Hamari, Jonna Koivisto, and Harri Sarsa. 2014. Does gamification work?–a literature review of empirical studies on gamification. In *2014 47th Hawaii international conference on system sciences*. Ieee, 3025–3034.

[20] Government Communications Headquarters. 2023. CyberFirst Girls Competition. Retrieved April 22, 2023 from https://www.ncsc.gov.uk/cyberfirst/girls-competition

[21] Solomon Hykes. 2013. Docker. https://www.docker.com/

[22] INDIRE. 2007. *Il profilo educativo, culturale e professionale (PECUP) (in Italian) - The Educational, Cultural, and Professional Profile (PECUP)*. Technical Report. Istituto Nazionale di Documentazione, Innovazione e Ricerca Educativa (INDIRE). https://www.indire.it/lucabas/lkmw_file/nuovi_tecnici/05_1_11_113_il%20profilo.pdf

[23] Istat 1926. Istituto nazionale di statistica. Retrieved May 2, 2023 from https://www.istat.it/

[24] Istat 2024. Resident population as of January 1st (in Italian). Retrieved July 19, 2024 from http://dati.istat.it/Index.aspx?DataSetCode=DCIS_POPRES1

[25] Monique M Jethwani, Nasir Memon, Won Seo, and Ariel Richer. 2017. "I Can Actually Be a Super Sleuth" Promising Practices for Engaging Adolescent Girls in Cybersecurity Education. *Journal of Educational Computing Research* 55, 1 (2017), 3–25.

[26] Lydia Koh. July 18, 2019. Cybersecurity competition for females in Singapore, CTF creates opportunity and diversity. Retrieved April 26, 2023 from https://theindependent.sg/cybersecurity-competition-for-females-in-singapore-ctf-creates-opportunity-and-diversity/

[27] Stela Kucek and Maria Leitner. 2020. An empirical survey of functions and configurations of open-source capture the flag (ctf) environments. *Journal of Network and Computer Applications* 151 (2020), 102470.

[28] Joscha Legewie and Thomas A DiPrete. 2014. The high school environment and the gender gap in science and engineering. *Sociology of Education* 87, 4 (2014), 259–280.

[29] Kees Leune and Salvatore J. Petrilli. 2017. Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. In *Proceedings of the 18th Annual Conference on Information Technology Education* (Rochester, New York, USA) *(SIGITE '17)*. Association for Computing Machinery, New York, NY, USA, 47–52. https://doi.org/10.1145/3125659.3125686

[30] Chengcheng Li and Rucha Kulkarni. 2016. Survey of cybersecurity education through gamification. In *2016 ASEE Annual Conference & Exposition*.

[31] LinuxServer.io 2021. Webtop. https://github.com/linuxserver/docker-webtop

[32] Rocío Lorenzo, Nicole Voigt, Miki Tsusaka, Matt Krentz, and Katie Abouzahr. 2018. How diverse leadership teams boost innovation. *Boston Consulting Group* 23 (2018), 112–134.

[33] Allison H Master and Andrew N Meltzoff. 2020. Cultural stereotypes and sense of belonging contribute to gender gaps in STEM. *Grantee Submission* 12, 1 (2020), 152–198.

[34] Lucas McDaniel, Erik Talvi, and Brian Hay. 2016. Capture the flag as cyber security introduction. In *2016 49th hawaii international conference on system sciences (hicss)*. IEEE, IEEE Computer Society, USA, 5479–5486.

[35] Maria Teresa Morana and Simonetta Sagramora. 2024. *Focus "Le carriere femminili in ambito accademico" (in Italian)*. Ministero dell'istruzione, Roma, RM, Italy. https://ustat.mur.gov.it/media/1276/focus_carrierefemminili_universit%C3%A0_marzo2024.pdf

[36] Fiona Fui-Hoon Nah, Qing Zeng, Venkata Rajasekhar Telaprolu, Abhishek Padmanabhuni Ayyappa, and Brenda Eschenbrenner. 2014. Gamification of education: a review of literature. In *HCI in Business: First International Conference, HCIB 2014, Held as Part of HCI International 2014, Heraklion, Crete, Greece, June 22-27, 2014. Proceedings 1*. Springer, Berlin, Germany, 401–409.

[37] Yuri Nesen, Brian Fowler, and Emiliana Vegas. 2021. *How Italy Implemented Its Computer Science Education Program*. Technical Report.

[38] Women's Society of Cyberjutsu. 2018. CGA Competition Teams. Retrieved April 26, 2023 from https://womenscyberjutsu.org/mpage/CGA_Team

[39] Charlie Osborne and Steve Morgan. 2022. Women in Cybersecurity 2022 Report. Retrieved April 29, 2023 from https://cybersecurityventures.com/wp-content/uploads/2022/09/Women-In-Cybersecurity-2022-Report-Final.pdf

[40] Francesca Palmini and Daniela Di Ascenzo. 2023. *Focus "Principali dati della scuola – Avvio Anno Scolastico 2023/2024" (in Italian) - Focus: "Main School Data – Start of the 2023/2024 School Year"*. Technical Report. Ministero dell'Istruzione e del Merito (MIUR). https://www.miur.gov.it/documents/20182/0/Principali+dati+della+scuola+-+Focus+avvio+anno+scolastico+2023-2024.pdf/8ba0c506-a14f-9071-fbb7-e0aede0a5ebb?t=1695388882235

[41] Elena Prieto-Rodriguez, Kristina Sincock, Regina Beretta, Karen Blackmore, Juanita Todd, Erica Wanless, Sarah John, and Anna Giacomini. 2022. Investigating the Impact of an Outreach Intervention on Girls' STEM Identity Formation. *International Journal of Gender, Science and Technology* 14, 2 (2022), 183–206.

[42] Catherine Riegle-Crumb and Karisma Morton. 2017. Gendered expectations: Examining how peers shape female students' intent to pursue STEM fields. *Frontiers in psychology* 8 (2017), 329.

[43] Cecilia Stajano and Elisabetta Gramatica. 2014. Coding Girls. Retrieved May 2, 2023 from https://www.mondodigitale.org/progetti/coding-girls

[44] Heidrun Stoeger, Xiaoju Duan, Sigrun Schirner, Teresa Greindl, and Albert Ziegler. 2013. The effectiveness of a one-year online mentoring program for girls in STEM. *Computers & Education* 69 (2013), 408–418.

[45] Edith Cowan University. 2022. Girls' Programming Network. Retrieved April 26, 2023 from https://www.ecu.edu.au/schools/science/events-and-activities/computing-and-security-discipline/girls-programming-network

[46] Alastair Janse van Rensburg and Richard Baker. 2021. *CTF EVENTS Contemporary Practices and State-of-the-Art in Capture-the-Flag Competitions*. Technical Report. European Union Agency for Cybersecurity (ENISA). https://www.enisa.europa.eu/publications/ctf-events

[47] Ming-Te Wang and Jessica L Degol. 2017. Gender gap in science, technology, engineering, and mathematics (STEM): Current knowledge, implications for practice, policy, and future directions. *Educational psychology review* 29 (2017), 119–140.

[48] Eric Yuan. 2011. Zoom. https://zoom.us/

[49] Saadia Zahidi. 2023. *Global Gender Gap Report 2023*. Technical Report. World Economic Forum. https://www.weforum.org/reports/global-gender-gap-report-2023/in-full/gender-gaps-in-the-workforce#gender-gaps-in-the-workforce