Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 9

11-13-2023

Building a Diverse Cybersecurity Workforce: A Study on Attracting Learners with Varied Educational Backgrounds

Mubashrah Saddiqa
Aalborg University, Denmark, mus@es.aau.dk

Kristian Helmer Kjær Larsen1 Helmer Kjær Larsen
Aalborg University, Denmark, khkl@es.aau.dk

Robert Nedergaard Nielsen
Aalborg University, Denmark, robertnn@es.aau.dk

Jens Myrup Pedersen
Aalborg University, Denmark, jens@es.aau.dk

Building a Diverse Cybersecurity Workforce: A Study on Attracting Learners with Varied Educational Backgrounds

Abstract

Cybersecurity has traditionally been perceived as a highly technical field, centered around hacking, programming, and network defense. However, this article contends that the scope of cybersecurity must transcend its technical confines to embrace a more inclusive approach. By incorporating various concepts such as privacy, data sharing, and ethics, cybersecurity can foster diversity among audiences with varying educational backgrounds, thereby cultivating a richer and more resilient security landscape. A more diverse cybersecurity workforce can provide a broader range of perspectives, experiences, and skills to address the complex and ever-evolving threats of the digital age. The research focuses on enhancing cybersecurity education to attract a diverse audience through the development and testing of a virtual platform on Haaukins (a cybersecurity training platform) designed with features resembling social media for capture-the-flag exercises. The results show that the cyber training platform effectively engages a diverse group of learners, bridging the gap between traditional technical boundaries and the urgent demand for comprehensive cybersecurity competence.

Keywords

Cybersecurity, Diversity, Privacy, Training Platform, High School Students

Cover Page Footnote

Acknowledgement We acknowledged Linda Mostrup Pedersen for workshops coordination, Arianna Sammarchi for data collection, the teachers for their insightful feedback, and Industriens Fond for the financial support. Credits author statement Mubashrah Saddiqa: Conceptualization, data collection, analysis, writing. Kristian Helmer Kjær Larsen: Conceptualization, workshop design and execution, exercise development, writing. Robert Nedergaard Nielsen: Conceptualization, workshop design and execution, exercise development, editing and review. Jens Myrup Pedersen: Conceptualization, editing and review, supervision.

Building a Diverse Cybersecurity Workforce: A Study on Attracting Learners with Varied Educational Backgrounds

Mubashrah Saddiqa
Electronic Systems Department
Aalborg University
Copenhagen, Denmark
mus@es.aau.dk
https://orcid.org/0000-0002-4816-2426

Kristian Helmer Kjær Larsen
Electronic Systems Department
Aalborg University
Copenhagen, Denmark
khkl@es.aau.dk
https://orcid.org/0009-0003-7996-5429

Robert Nedergaard Nielsen
Electronic Systems Department
Aalborg University
Copenhagen, Denmark
robertnn@es.aau.dk
https://orcid.org/0000-0001-6356-8072

Jens Myrup Pedersen
Electronic Systems Department
Aalborg University
Copenhagen, Denmark
jens@es.aau.dk
https://orcid.org/0000-0002-1903-2921

***Abstract*— Cybersecurity has traditionally been perceived as a highly technical field, centered around hacking, programming, and network defense. However, this article contends that the scope of cybersecurity must transcend its technical confines to embrace a more inclusive approach. By incorporating various concepts such as privacy, data sharing, and ethics, cybersecurity can foster diversity among audiences with varying educational backgrounds, thereby cultivating a richer and more resilient security landscape. A more diverse cybersecurity workforce can provide a broader range of perspectives, experiences, and skills to address the complex and ever-evolving threats of the digital age. The research focuses on enhancing cybersecurity education to attract a diverse audience through the development and testing of a virtual platform on Haaukins (a cybersecurity training platform) designed with features resembling social media for capture-the-flag exercises. The results show that the cyber training platform effectively engages a diverse group of learners, bridging the gap between traditional technical boundaries and the urgent demand for comprehensive cybersecurity competence.**

Keywords— Cybersecurity, Diversity, Privacy, Training Platform, High School Students

I. Introduction

Cybersecurity has become an increasingly critical issue in today's digital age. An ever-growing number of online threats and attacks pose significant risks to individuals, organizations, and society. Yet, despite the urgent demand for adept professionals in this domain, a significant shortfall of cybersecurity experts persists. According to International Information System Security Certification Consortium (ISC)2 [1, 2], the shortage of cybersecurity professionals surpassed 3.4 million in 2022.

This shortage is particularly acute in terms of diversity, with women, people of color, expertise, and skills [3, 4]. The need for a diverse and inclusive cybersecurity workforce is not only a matter of social justice and equity but is also essential for addressing the complex and evolving challenges of cybersecurity in today's world. Research has shown that a lack of diversity in cybersecurity can lead to blind spots in threat detection and slower response times to emerging threats [5, 6].

In the digital age, embracing diversity is crucial for effectively addressing the complex and ever-evolving threats to our safety and security [7]. Excluding different perspectives and diverse representation from various educational backgrounds limits our ability to tackle current challenges and prepare for future threats [8]. With digitalization impacting every aspect of our lives, it is imperative to find creative and global solutions to address the growing scale and complexity of threats [9]. Diversity is an essential tool in our collective toolkit, fostering more robust, innovative, and agile ideas [10].

The research in this article focuses on diversity from an educational background perspective, encompassing a variety of technical and non-technical backgrounds. We use the term 'diversity' to include various educational backgrounds [11], including both technical and non-technical education, as well as promoting women's representation. This research investigates how to attract a more diverse audience to cybersecurity by incorporating broader concepts and developing engaging Capture-The-Flag (CTF) exercises that align with the learners' educational backgrounds and goals. We will address the following research question,

"How can cybersecurity education be designed to appeal to a diverse range of learners, incorporating broader concepts such as data sharing, privacy, and ethics, and developing engaging capture-the-flag exercises that align with learners' educational backgrounds and goals?"

The research work is part of Danish Cyberskills project (https://www.cyberskills.dk/), which is a joint initiative by the public and private sectors to improve the country's cybersecurity workforce. The research work builds upon previous work [12] in which pre-developed capture-the-flag exercises on the Haaukins platform [13] were tested. These exercises focused on the topics of privacy, data sharing, and ethics and were tested with high school students with diverse educational backgrounds.

The findings from the previous work highlighted a need for exercises that cater to the students' level of understanding, particularly those without a technical background. Building on these insights, we developed a virtual platform similar to social media platform within Haaukins containing capture-the-flag exercises that emphasized broader concepts of cybersecurity. We then tested this platform with a diverse group of learners, including those with technical and non-technical backgrounds.

In the subsequent sections, we will provide a more detailed description of our research methods, findings, and the implications for cybersecurity education. Specifically, Section 2 will provide background information on the importance of cybersecurity and the need for a more diverse workforce. Section 3 outlines methodology for developing and testing the capture-the-flag exercises on the Peacock platform while Section 4 will provide an overview to Peacock platform (a virtual training platform resembles social media) with CTF exercises. Finally, Sections 5 and 6 will present our findings and generalization of the results while Section 7 concludes the paper.

II. BACKGROUND

While the demand for a more diverse cybersecurity workforce is paramount, the surge in social media use, gaming, and digital platforms underscores the importance of instilling comprehensive cybersecurity concepts. The integration of broader notions like privacy, data sharing, and ethics is particularly critical among the younger generation, who are frequent users of these platforms [14].

Bringing diversity into the cybersecurity field and helping young people navigate social media are interconnected challenges that require a solution. These threats affect not only adults but also impact young people, who may be more vulnerable due to their limited understanding of online privacy and security [15]. As we work to create a more inclusive workforce in cybersecurity, we must simultaneously consider the needs and vulnerabilities of the diverse user base, particularly the youth who are immersed in the digital realm [16]. Hence, while fostering diversity within the cybersecurity workforce, we must also empower young individuals with essential knowledge about online safety, privacy, and responsible digital behavior.

By incorporating cybersecurity education that emphasizes diverse concepts such as privacy, data sharing, and ethics, we can empower young people to protect themselves and their data online. For instance, understanding the importance of privacy can help young people recognize the risks associated with sharing personal information online, and taking steps to protect their privacy [17]. Similarly, introducing the notion of data sharing can help young people become more aware of how their personal data is collected, used, and shared online [18]. The introduction of these concepts to a diverse audience can facilitate the creation of a more robust and innovative cybersecurity workforce, equipped to effectively combat the evolving digital threats of our time.

One of the biggest challenges in attracting a more diverse workforce in cybersecurity is the lack of awareness and education about the field [9]. Many individuals may not even know that cybersecurity is a viable career option or may have misconceptions about the field. Additionally, traditional educational pathways into cybersecurity often require technical degrees or certifications, which can be a barrier for those without a technical background. This narrow view can limit the talent pool and prevent innovative ideas and solutions [19]. Overall, there is a need to broaden the perception of what it means to be a cybersecurity professional, increase awareness of the variety of career paths available, and foster a more inclusive and supportive environment that encourages individuals from diverse educational backgrounds to pursue careers in the field [3].

There are many ongoing projects in Europe aiming to address these challenges. The European Union Agency for Cybersecurity (ENISA) (https://www.enisa.europa.eu/) offers a variety of resources and initiatives aimed at improving cybersecurity education and awareness, including guidelines for teachers and an online platform for cybersecurity education. The EU's Horizon research and innovation program (https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en) includes funding for cybersecurity projects that address societal challenges, such as privacy and data protection.

Similarly, in Denmark efforts to address the need for a more diverse and skilled cybersecurity workforce Denmark include the CyberSkills project (https://www.cyberskills.dk/), which aims to enhance the digital competencies of the Danish workforce and increase the number of professionals with cybersecurity skills. The project focuses on promoting a diverse range of educational backgrounds and career paths to attract a wider range of individuals to the field. Other initiatives in Denmark include the establishment of the Danish Center for Cybersecurity (CFCS) (https://www.cfcs.dk/en/) which is part of Danish Defense Intelligence Services serves as a hub for public and private organizations to collaborate on cybersecurity issues and share knowledge and expertise. The CFCS also offers various training and education programs to enhance the cybersecurity skills of professionals in Denmark.

III. METHODOLOGY

In this research study, we employed a mixed-method approach to comprehensively investigate our research question, combining qualitative methods such as workshops, observations, and interviews, along with potential quantitative elements, to gain a deeper understanding of the diverse experiences and perspectives of high school students in the context of cybersecurity education.

A. *Participants Details*

Participants were selected from a variety of high schools, including STX, HTX, and HHX, using a random sampling method. In the previous research paper [12], details were provided about the Danish high school system. The Danish high school system comprises of four distinct types of high schools (https://eng.uvm.dk/upper-secondary-education/national-upper-secondary-education-programmes). For our study, we approached STX, HHX, and HTX high schools. These schools offer specialized education in a wide range of subjects, with STX focusing on general education, HHX catering to business-

oriented subjects, and HTX specializing in technical and scientific disciplines.

We engaged a diverse group with varying backgrounds, including technical disciplines like mathematics and programming, as well as non-technical fields like business management, music, humanities, and art, through interactive workshops. The participants were recruited by contacting teachers from different high schools, both those with technical and non-technical subjects, to organize and conduct the workshops. The interested teachers provided suitable dates and times, and the entire high school classes participated in the workshops. To cultivate a more inclusive audience, our approach involved engaging high school students across various subjects, with a particular emphasis on fields where female representation is relatively higher. By adopting this strategy, we aimed to enhance the understanding of cybersecurity concepts among women, who are currently underrepresented in this field. Participant details are provided in TABLE I.

TABLE I. PARTICIPANTS DETAILS

Schools Name	***Background***	***Workshop***	***Participants***	***City***
Handel Skole	Non-technical	12	300	Aalborg
Business Skole	Mixed	7	120	Aarhus
State Gymnasium	Non-technical	4	98	Aarhus
HTX Tradium	Mixed	1	25	Randers
Det Blå Gymnasium	Non-technical	4	73	Haderslev
Baltorp Gymnasium	Non-technical	1	23	Copenhagen
Learnmark HTX	Technical	1	25	Horsens
Aarhus Gymnasium	Technical	3	108	Aarhus

A total of 33 workshops were conducted across various cities in Denmark, with over 700 students participating (494 with non-technical, 133 with technical, and 145 with a mixed background). 17 teachers also participated in these workshops.

These workshops were specifically tailored for high school students, aiming to introduce them to broader concepts of cybersecurity. To gain insight into the perspectives and challenges faced in incorporating these concepts, short interviews and observations were conducted with both the students and their teachers.

Several ethical precautions have been taken to ensure the safety and confidentiality of participants in the research project. An information letter was sent to teachers outlining the research project and the activities conducted during the workshops. All data collected from participants were carefully anonymized, which means that individual identities cannot be traced. No sensitive or confidential information was shared during the research activities, and participants were not exposed to any risks or vulnerabilities. The data for this research was collected prior to the institution's implementation of a formal ethical approval process for research. However, during the data collection period, we adhered to ethical principles and guidelines that were in effect at that time to ensure the privacy and well-being of participants.

The following subsections provide a comprehensive overview of the workshop design, as well as a description of the methodology employed during the interviews and observations.

B. *Design for workshop*

The workshops are divided into two main parts and have a duration of 3 hours. The first part is a presentation (30-40 minutes) that consists of an introduction to the cybersecurity, basic principles of the privacy, data sharing and ethics and several types of hackers. The second part consists of an active learning environment, where students are introduced to the Haaukins. In this part of the workshop the students will have to work with the CTF exercises from the Peacock platform (virtual social media for cyber training) in groups. The facilitator will help students if they are stuck and facilitate their learning process throughout the journey from getting started with solving the CTF exercises to finding relevant information on the needed tools.

C. *Observations*

During the workshops, we conducted detailed observations of the students' level of interest in the subject and their performance while working on various CTF exercises. We paid close attention to the areas where they encountered difficulties, identified topics that appealed to them the most, and took note of exercises they found challenging.

D. *Interviews*

In addition, we conducted brief interviews with the students to gain insight into their perspectives on the broader concepts of cybersecurity and how we can make it more engaging for them. Out of 772 students, approximately 200 female and 280 male students participated in group interviews, with 3-4 students working together at each table. They represents a diverse range of educational backgrounds, with 280 students having non-technical backgrounds, 121 students from mixed backgrounds, and 49 students with technical expertise. The participants came from various locations, including Copenhagen, Aarhus, and Aalborg, spanning a wide geographical area within Denmark. We sought their opinions on ways to enhance their interest in the subject matter. Furthermore, we asked specific questions related to the different exercises to assess the extent to which the intended learning goals were achieved. Additionally, we encouraged the students to provide input and suggestions for creating new exercises, fostering a collaborative approach in the development of innovative learning materials.

At the end of the workshop, participants had the opportunity to share their feedback through an online survey, including their thoughts on the Peacock exercises and their overall experience of the workshop.

IV. Peacock platform (a virtual training platform resembles social media) for CTF Exercises

The Peacock Platform has been developed as part of this research study and builds upon and addresses the findings of previous research work [12]. It serves as a continuation of the previous research, aiming to further explore and address the identified gaps and challenges.

Peacock resembles a social media platform integrated into the privacy universe part of the Haaukins. Haaukins is a cybersecurity training platform developed by Aalborg University that provides participants with a secure virtual environment where they can engage in a wide range of cybersecurity CTF exercises [13]. These exercises cover diverse areas such as network forensics, web exploitation, reverse engineering, binaries, cryptography, and privacy. The platform's automated setup simplifies the creation and deployment of lab environments, enabling participants to effectively practice their skills. By utilizing Haaukins, individuals can enhance their cybersecurity proficiency through hands-on experiences and practical exercises. Each individual or team interacts with their own instance of the platform, ensuring that nothing is shared between users. Peacock, as a component of Haaukins, specifically focuses on privacy-related aspects within the social media realm, further enriching the training experience.

The graphical design of the platform draws inspiration from popular social media platforms such as TikTok, Instagram and Facebook as shown in Fig. 1. The set of CTF exercises focuses on incorporating the privacy concept and OSINT (open-source intelligence) into an easily approachable set of exercises for complete beginners. The main idea behind these exercises is to gradually introduce students to the privacy and OSINT concept on social media without prior technical knowledge and skills in it.

The exercises have been designed with a progression, initially requiring no tools, followed by gradually introducing users to different tools and methods, one at a time. To facilitate the learning process for students, a PDF file (toolbox) has been created, that encompasses details of all the necessary tools for solving the exercises. The toolbox's main aim is to provide students with a starting point for addressing diverse exercises and acquainting them with the usage of terminal commands.

A total of 11 exercises have been developed for the platform, as outlined in TABLE II. A concise description of each exercise is also provided in TABLE II. The difficulty levels encompass both easy and medium exercises. An easy exercise typically requires 1-3 steps for completion, while a medium exercise entails 3-5 steps. A short description of these exercises is given below.

1. Anonymous Sandworms 1

The main idea behind this exercise is to teach the students about how the different interactions between users on a social media platform can be abused to infer relationships and personal information that has not been directly shared by a user.

TABLE II. Peacock Platform exercises overview

Sr. No.	*Name*	*Category*	*Difficulty*
1.	Anonymous Sandworms 1	OSINT	Easy
2.	Anonymous Sandworms 2	OSINT	Easy
3.	Anonymous Sandworms 3	OSINT	Easy
4.	The Golden Seagull	OSINT	Easy
5.	The Cultural Code	OSINT	Easy
6.	The Yellow Snitch	OSINT	Easy
7.	Johns Weird Comment!	OSINT	Easy
8.	The Hash Hack	Forensics	Medium
9.	Rockies Code	OSINT	Easy
10.	The Graduation Party	OSINT	Easy
11.	The Suitcase	Forensics	Medium

In this exercise, students start by closely observing interactions between users on a social media platform and employing a straightforward stalking technique to identify indirect disclosures of personal information. Once they identify such instances, they proceed to analyze the data, drawing conclusions about the relationships between users and collecting information that may not have been shared directly. Finally, they submit their findings in the form of flag format.

2. Anonymous Sandworms 2

It is not always through text that we share information. This exercise deals with the images we share and the information that appears visually on them. Therefore, it is also important to be aware of the information that we share through the images that we share on social media or the like. For example, visual information that can be used to find out where we are.

3. Anonymous Sandworms 3

This exercise revolves around the information we share while interacting on social media platforms or similar ones. It builds upon what students have learned in the first two exercises. This time, rather than focusing on relationships, students will attempt to misuse the information they've gathered to gain access to another user's profile, including their email and password. The goal is to teach students to 'think like a hacker,' not in the sense of 'acting like a hacker,' but to help them learn how to better protect themselves.

4. The Golden Seagull

In this exercise, the focus is on understanding what information is embedded in the images that users share. To solve the exercise students must gain basic knowledge on what types of data can be embedded in pictures, some of which can be abused in different contexts.

5. The Cultural code

Some information can be shared, without necessarily being in human readable form. In this exercise, the students must

utilize this by reading data from a picture in a widely used format.

6. The Yellow Snitch

Useful information is usually written down on post-it notes in office environments. This exercise focuses on the abuse of these when pictures of a workspace is shared. The exercise shows some of the risks involved in sharing images that contain personal information.

7. Johns Weird Comment

This exercise touches upon a more technical subject. Namely that useful information is not always shared in clear text but is sometimes found in encoded format. The students are expected to find and decode an encoded message from the platform to solve the exercise.

8. The Hash Hack

Passwords are usually encrypted with a hashing algorithm or similar when they are stored on websites. Some algorithms are more secure than others. In this exercise, students examine a hash generated from a common hashing algorithm and find out that it has several weaknesses, which is why other algorithms are used in new systems to store passwords.

9. The Suitcase

This exercise focusses on the fact that malicious files can be embedded in pictures or the like. To solve this exercise, students get acquainted with a common forensics tool for analyzing files to solve this exercise.

10. Rockies Code

This exercise is a sister exercise to "The Yellow Snitch" combined with "The Hash Hack". In this exercise students will combine principles from OSINT and hashing algorithms gained from the mentioned exercise and use them in a new context.

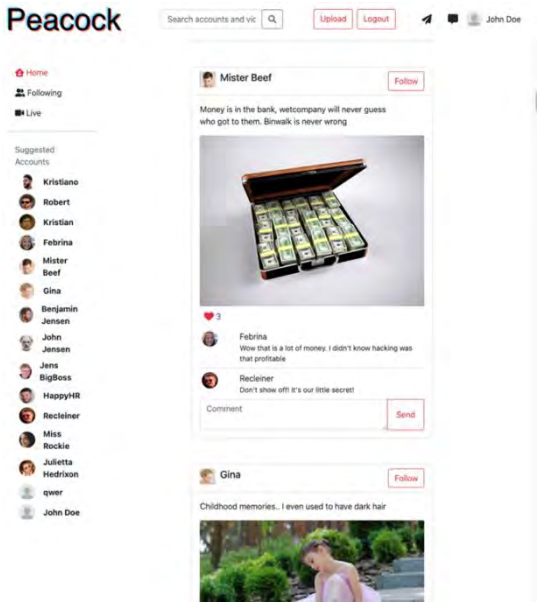

Fig. 1. Overview of Peacock platform on Haaukins

11. The Graduation Party

This exercise is a sister exercise to "The Yellow Snitch" but the information shared has another sensitive character. The methodology is the same as the one in "The Yellow Snitch", but the context is different.

A. *Learning goals Associated with the Peacock Exercises:*

After solving the exercises included on the peacock social media platform the student will be able to:

1. Understand different privacy and ethics related cybersecurity aspects of sharing data on social media. By achieving this learning goal, individuals will be equipped with the necessary knowledge to make informed decisions about what information to share. This includes gaining knowledge about the potential risks and vulnerabilities that arise from sharing personal information online and recognizing the importance of protecting sensitive data.
2. To use some of the basic tools used in forensics for cybersecurity including basic terminal commands and tools. The objective of this learning goal is to develop practical skills in using fundamental tools employed in cybersecurity forensics. Participants will learn basic terminal commands and tools that are commonly used in analyzing and investigating cyber threats and incidents.
3. Understand the different data types that can be abused by cyber criminals on social media platforms. This learning goal aims to enhance awareness and comprehension of the diverse types of data that can be exploited by cybercriminals on social media platforms. Participants will gain knowledge about sensitive information such as personally identifiable information (PII), geolocation data, and behavioral patterns that can be targeted by cybercriminals for malicious activities like identity theft, phishing attacks, and social engineering.

V. Results

In this section, we will analyze and discuss the findings obtained from the study. The primary objective is to provide a comprehensive overview of the collected data, emphasizing significant observations and outcomes. Overall, 772 students participated in the research study, where 565 students also provide their feedback through online survey. Out of 772 students, 407 (52%) were male, 356 (46%) women, and 9 (1%) under others category. Data gathered from a diverse group of participants using short interviews, observation, and an online survey to answer our research question. Around 540 students answered the online survey while 480 also participated in short interviews. The analysis of this data revealed several main themes, each with its own sub-themes. In the following sections, we will discuss these main themes and their corresponding sub-themes in detail.

A. *The effectiveness of incorporating broader concepts into cybersecurity education*

During the workshops, we conducted short interviews with both teachers and students to gather data about the inclusion of broader cybersecurity concepts such as privacy, data sharing and ethics etc. Teachers' perspectives on integrating broader cybersecurity concepts into the curriculum are foundational. All 17 participating teachers supported the integration of these concepts. They believe that introducing broader ideas like privacy, data sharing, and ethics would be engaging for students, as these concepts relate to their everyday lives. For instance, students can understand the importance of strong passwords and the ease of guessing passwords based on shared online information. These results indicate that adding these ideas to cybersecurity education can help students bridge theory and real-life scenarios. Therefore, integrating broader concepts offers valuable prospects not only for individuals with technical backgrounds but also for those with non-technical backgrounds to comprehend diverse aspects of cybersecurity and explore careers in the field. One of the participant teachers said:

"In today's digital age, it's important to know how to stay safe when you're online. By including broader cybersecurity concepts in education, we can give young people the skills they need to navigate the digital world securely. Also, many students are not even aware of these concepts, so introducing them in education can also help in generating their interest and curiosity about cybersecurity." (Participant Teacher 1, Nov 2022)

For interviews with the students, we selected participants through a random sampling approach, targeting students who were willing to participate in our study. For instance, we conducted interviews with a diverse group of female students to gain insight into their perspectives on cybersecurity. Female participants provided insightful feedback, expressing a strong positive response to the cybersecurity content. They found the subject genuinely interesting, in contrast to the common perception that it can be both boring and overly technical.

Similarly, students with technical backgrounds were interviewed to understand the relevance of broader cybersecurity concepts, regardless of their technical expertise. They generally appreciated the inclusion of comprehensive topics in their education.

By expanding the scope of cybersecurity education, students can be empowered to enhance their proficiency in digital technologies and social media platforms. Moreover, the inclusion of these topics in education facilitates increased awareness among young individuals regarding diverse forms of cyberattacks, thereby enabling them to navigate the digital landscape more effectively.

Overall, the incorporation of broader concepts of cybersecurity into educational curricula is regarded as intriguing by the participants (both students and teachers).

Integrating broader cybersecurity concepts can have a two-way impact. First, it sparks more interest to a diverse audience with various educational background by relating the subject to students' lives, encouraging them to get more involved. Second, this increased interest leads to more focused learning, helping them understand the concepts better and improving their overall knowledge and awareness. The results within this category are further divided into the following sub-sections, which are described below.

1) *Increased Interest*

The feedback received from students who participated in the short interviews during the workshops underscores their heightened interest and active engagement in the broader concepts of cybersecurity, including privacy, ethics, data sharing, and the utilization of social media. This inclusive approach empowers students from diverse academic backgrounds, encompassing the social sciences, arts, and humanities, to contribute meaningfully to the domain of cybersecurity.

Fig. 2 represents participants' response about the peacock exercises where the majority find these exercises interesting. Students value the interdisciplinary nature of the educational approach, as it broadens their understanding of the societal impact associated with cybersecurity and encourages the cultivation of critical thinking skills in addressing cyber threats. Notably, students exhibited high levels of engagement and motivation when engaging in CTF exercises during the workshops. One of the participants said:

"Before attending the workshop, I thought it might be boring, but I ended up finding the topic interesting. What stood out to me the most were the real-life examples used to explain different types of cyber threats and attacks." (Participant 1, Dec 2022)

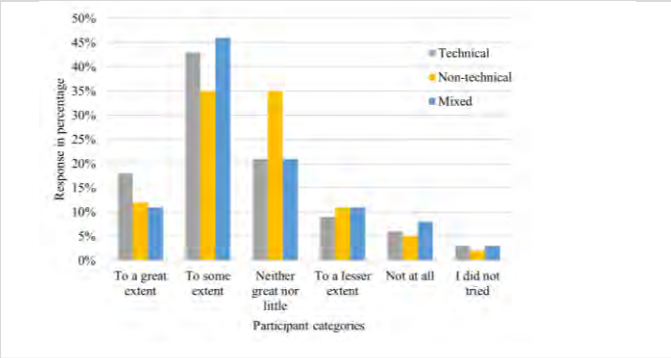

Fig. 2. Participants response about "Did you find Peacock exercises interesting?"

According to the insights shared by the teachers during the interviews, it is suggested that to effectively engage a more diverse audience in the field of cybersecurity, early exposure to broader concepts becomes essential. By introducing these broader concepts during the initial stages of education, students can develop a comprehensive understanding of the subject matter and be better equipped to explore future opportunities. This proactive approach is deemed crucial in promoting inclusivity and ensuring equitable access to cybersecurity education and subsequent career prospects for individuals from diverse backgrounds.

2) *Improved Digital Literacy and Awareness*

During the workshops, students actively engaged in solving the CTF exercise. They eager to learn and use different tools to solve different exercise. This shows that integrating broader

concepts into cybersecurity education can help equip young individuals with the necessary knowledge to navigate the digital landscape effectively. By understanding the risks associated with online social media platforms and technologies, students can make informed decisions and employ appropriate security measures to protect their digital assets. One of the participants said:

"The presentation and privacy exercises made me see things differently. Now I understand the importance of being mindful before sharing anything on social media. As someone who's always active on those platforms, it's become clear to me that I need to think twice and take steps to protect my privacy." (Participant 2, Dec 2022)

Another participant said:

"Today's workshop was helpful in helping me understand different types of cyber-attacks better. I had heard of phishing and social engineering before, but today, when I heard real-life examples shared during the workshop, everything became much clearer to me." (Participant 3, Feb 2023)

This also enhances their ability to identify and respond to various types of cyberattacks, including phishing, social engineering, and malware.

B. *Feedback on Peacock Exercises*

During the workshop, participants were initially introduced to the fundamental concepts of cybersecurity, followed by engaging in hands-on CTF exercises using the Peacock platform on Haaukins. The purpose of these exercises was to establish a connection between the broader concepts and their real-life applications. By offering an interactive experience, the intention was to present cybersecurity as an intriguing and enjoyable subject, thus attracting a wider audience. To ensure continuous improvement, it is essential to solicit feedback from the students regarding these exercises. This feedback will play a vital role in identifying areas that require enhancement and making the exercises more captivating. The following subsections will encompass the overall feedback received for different exercises, strategies for enhancing exercise design, and an assessment of whether the learning objectives were successfully achieved through the completion of these exercises.

1) General Feedback on Peacock Exercises

Overall, the Peacock exercises were well-received by students, with some of them becoming so engaged that they continued to solve exercises even after the workshop. The participants generally liked the Peacock platform, which is a social media platform for training, where different profiles are created. To solve an exercise, students had to carefully read the descriptions of various tasks and find the required information to locate a flag and earn points. The exercises started off simple and gradually increased in difficulty. Students worked with tools such as Google Maps, Exif (Exchangeable Image File Format), Binwalk (a command-line tool used for analyzing binary files, particularly firmware images, to extract embedded files), hashing, and decoding tools. One of the participant teachers provide his feedback about Peacock exercises as:

"The Peacock challenges are a great way to engage students without a technical background in cybersecurity. These challenges capture their interest because they involve tasks that they are already familiar with, making them more enjoyable and relatable." (Participant Teacher 2, Dec 2022)

Another participant said regarding the exercises:

"Starting the task and finding the first hint may be challenging, but once you do, it becomes really interesting." (Participant 4, Feb 2023)

The feedback from the online survey shows that many of the students enjoyed solving the Peacock exercises as shown in Fig. 3.

2) Suggestions for Improving the Design and Implementation of Peacock Exercises

Participants appreciated the exercises design and descriptions but encountered some difficulties in understanding certain descriptions. For instance, the flag format for "Anonymous sandworms 2" differed from that of "Anonymous sandworms 1," as it required the use of lowercase letters, which was different from the first exercise. Students also found the "Cultural Code" exercise interesting but were confused by the description, as they were uncertain about the specific type of information they needed to provide as a flag.

The students feedback about "How helpful were the hint in the description of the Peacock exercises?" is shown in Fig. 4. Most students with technical backgrounds found the exercise descriptions very helpful, while students with non-technical and mixed educational backgrounds initially found the exercises description to be challenging. Nevertheless, after becoming familiar with the exercises, they also found the exercises description and hints to be helpful in solving the exercises.

Additionally, students without a technical background found exercises involving tools like EXIF and Binwalk challenging. After conducting the initial Peacock workshops, a cheat sheet toolbox guide was created. This guide provides students with hints on using various tools (e.g., Exif, Binwalk etc.), helping to keep them motivated. Students had no issues working with Haaukins where the Peacock platform is integrated with ambassador support, but they suggested the creation of a brief walkthrough video to explain the different features of Haaukins for future reference.

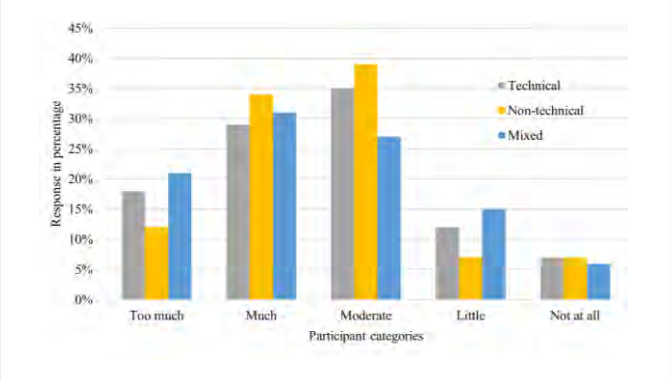

Fig. 3. Participants response about "Did you enjoy solving the Peacock exercises?"

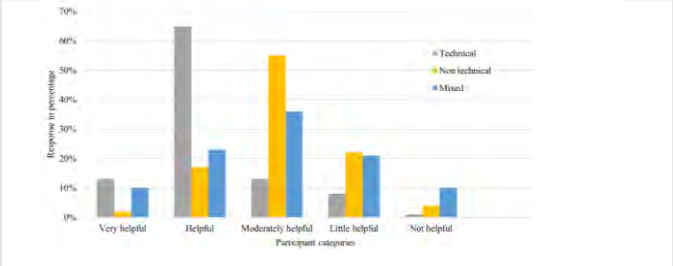

Fig. 4. Participants response about *"How helpful were the hints in the description of the Peacock challenges"?*

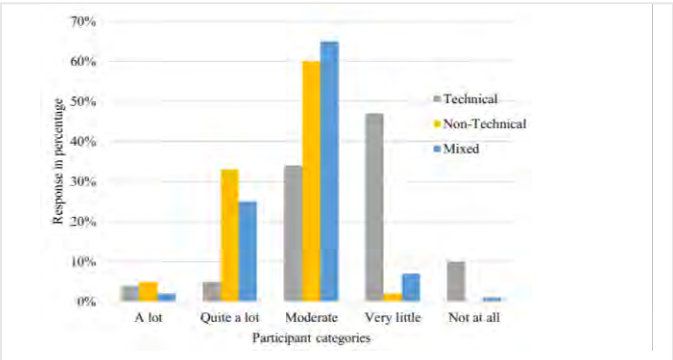

Fig. 5. Participants response about "Did you need help in solving Peacock challenges"?

Several technical issues were also observed that could improve and enhance the user experience. For instance, MacBook users found it slightly challenging to switch between their own keyboard layout and Linux keyboard layout to solve tasks.

Therefore, providing them with shortcut keys for copying and pasting would greatly facilitate them in navigating the platform. The students' feedback about "did you need help in solving Peacock exercises" is shown in Fig. 5.

The results indicate that a number of participants, particularly those from a non-technical background, expressed a need for assistance when solving the exercises. The varying levels of assistance needed can be attributed to the varying degrees of technical knowledge and familiarity with cybersecurity concepts among the participants.

3) Evaluation of Learning Outcomes of Peacock Exercises

The Peacock platform offers a set of exercises designed to facilitate learning outcomes related to privacy, OSINT, and cybersecurity in the context of social media. During the workshop, we observed and did short interviews with the students to evaluate the learning outcomes associated with these exercises. A brief description is given below:

a) *Understanding different privacy-related cybersecurity aspects of sharing data on social media*

Students demonstrated a solid understanding of privacy risks and vulnerabilities associated with sharing personal information on social media platforms. Many students were able to make informed decisions about what information to share on social media, considering the potential risks involved. Students also showed a high level of awareness regarding the

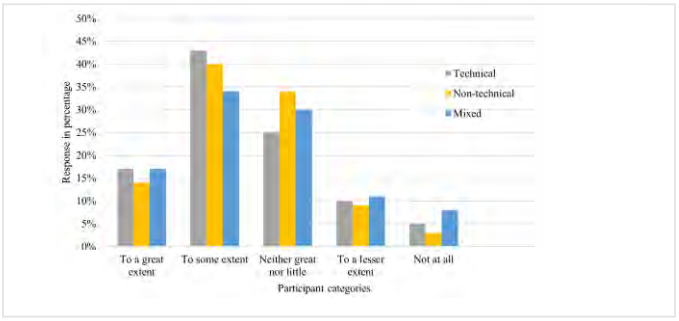

Fig. 6. Participants response about "Did the Peacock exercises help in understanding privacy concepts when you are online"?

importance of protecting sensitive data and were able to identify ways to safeguard their information online. When we asked one of the participants what they learned from today's workshop, he said:

"After completing the cultural code exercise, I realized how vital it is to prioritize privacy when we're online. Sharing anything you want can be very risky and unsafe." (Participant 5, Feb 2023)

Fig. 6 represents the participants' responses regarding the effectiveness of the Peacock exercise in understanding privacy concepts when online. The results indicate that a majority of participants found the Peacock exercise helpful in understanding privacy concepts. However, a significant number of participants indicated that the exercises were either not very helpful or only helped to a lesser extent in understanding privacy concepts. One possible explanation for this discrepancy could be the abstract nature of the topic, particularly for non-technical individuals. Privacy concepts in the online realm can be complex and challenging to grasp, especially for those without a strong technical background or prior knowledge in cybersecurity.

To improve the learning experience for non-technical students, it would be beneficial to incorporate more tangible and relatable examples and use plain language to explain complex terms. Additionally, demonstrating the direct impact of privacy concerns on personal lives can make the topic more accessible and relevant.

b) *Using basic tools in forensics for cybersecurity, including terminal commands and tools*

Many students were able to apply the acquired knowledge to analyze and investigate cyber threats and incidents using the provided tools. Students demonstrated a satisfactory level of familiarity with the basic tools used in the field of cybersecurity forensics. However, some students also faced challenges due to the technical complexity of the tools and required additional support to fully grasp their usage. One of the participants said:

"At the beginning, it was challenging for me to grasp the instructions and navigate the tools needed to solve the exercise. However, with the help of the internet and the support from the ambassadors, I now feel more confident in using them, at least at a beginner level." (Participant 6, Apr 2023)

c) *Understanding the different data types that can be abused by cybercriminals on social media platforms*

The observation during the workshops reveals that students exhibited a strong comprehension of various data types that can be exploited by cybercriminals on social media platforms. Students showed a clear understanding of sensitive information such as personally identifiable information (PII), geolocation data, and behavioral patterns that can be targeted by cybercriminals for malicious activities. Students displayed a high level of awareness regarding the risks associated with the misuse of different data types on social media platforms and were able to identify potential threats and vulnerabilities. Here is a participant's thought:

"I was amazed to learn how easily someone can find out about us using our location information. It's important to be careful about sharing where we are online. I also found it surprising that hackers can hide information in images or files to get access to our personal data. It's a reminder to be cautious and think about what we share online." (Participant 7, Apr 2023)

Overall, the results indicate that the exercises provided on the Peacock platform effectively facilitated the achievement of the intended learning outcomes. The students successfully developed a comprehensive understanding of privacy-related cybersecurity aspects, gained practical skills in using forensics tools, and enhanced their awareness of data types that can be exploited by cybercriminals.

However, the evaluation also identified several hurdles that impacted the achievement of the desired outcomes. Technical complexity emerged as a challenge, particularly for students with limited prior knowledge in cybersecurity and forensics. Time constraints also affected students' ability to delve deeper into the exercises, compromising the depth of understanding and skill development for some. Limited resources and access to necessary tools presented additional hurdles for certain students. The breadth of topics covered in the exercises, ranging from privacy concerns to different types of data exploitation, may have resulted in information overload for some students with non-technical backgrounds. Absorbing and retaining a significant amount of information within a limited timeframe have been challenging for some of the students with no prior knowledge.

C. *Barriers and Challenges in Attracting Diverse Audience:*

During the workshops, we also posed questions to students to identify the barriers in engaging a diverse audience with varying educational backgrounds in cybersecurity. The results are listed below.

1) Lack of Awareness

The short interviews and workshop observations reveal that participants without technical backgrounds often lack awareness of cybersecurity opportunities. Many students perceive cybersecurity as a technically complex domain, closely tied to coding skills. To attract a diverse audience, it's crucial to address these misconceptions and emphasize the wide range of careers within cybersecurity. Connecting cybersecurity to students' interests, such as medicine for those inclined toward the medical field, can help bridge gaps and underscore the field's interdisciplinary character.

2) Lack of Representation

The lack of representation within the cybersecurity field is also identified as a significant barrier according to the data collected through short interviews with students. Students need to see individuals who resemble them or share similar backgrounds participating in cybersecurity-related activities. This representation serves as an inspiration and demonstrates that anyone, regardless of their educational background, can excel in cybersecurity. By highlighting diverse role models and showcasing their achievements, we can inspire more students to consider cybersecurity as a viable career path.

3) Cultural Challenges

When discussing the possibility of pursuing cybersecurity as a future career or education, many female participants express doubts, perceiving it as something not meant for them. Addressing cultural challenges is crucial in overcoming this barrier. Having strong female role models who have succeeded in the field can serve as inspiration and can encourage more women to pursue careers in cybersecurity. Creating a supportive and inclusive environment that values diversity and actively promotes equal opportunities can help overcome cultural barriers and attract a more diverse talent pool to cybersecurity.

4) Limited Prominence and Perception of Cybersecurity

Another significant barrier identified during the research study is to attract a diverse audience to cybersecurity is the limited prominence and perception of the field. Promoting cybersecurity from early education is crucial to provide students with a better understanding of the subject when choosing their subjects in high school and beyond. It is essential to present cybersecurity as an interesting and enjoyable discipline rather than solely focusing on its technical aspects. One effective approach is organizing CTF competitions that cater to a diverse audience and incorporate broader concepts of cybersecurity, such as privacy, data sharing, and social media. These competitions can serve as interactive and engaging platforms to spark interest and demonstrate the practical and relevant aspects of cybersecurity. By emphasizing the broader implications and real-world applications of cybersecurity, we can generate curiosity and enthusiasm among students, encouraging them to explore the field further.

VI. Generalization and Implications

The results of this study can be generalized to broader contexts and applied to cybersecurity education initiatives. The effectiveness of the Peacock Social Media platform in introducing high school students to privacy, data sharing, and ethics suggests that similar approaches can be employed to engage learners with diverse educational backgrounds. By incorporating broader concepts and developing interactive learning experiences, cybersecurity education programs can attract a wider range of participants and promote inclusivity.

The findings of this study also highlight the importance of addressing the shortage of cybersecurity experts, particularly from diverse groups. The success of the Peacock platform in fostering interest and improving digital literacy among students

indicates that similar initiatives can be implemented to bridge the skills gap and encourage individuals from various backgrounds to pursue careers in cybersecurity.

Overall, the research demonstrates that the Peacock platform's approach to cybersecurity education can be generalized and adapted according to specific needs. By tailoring educational content and providing user-friendly experiences, similar platforms and programs can be developed to effectively train a more diverse cybersecurity workforce and address the challenges posed by cyber threats.

VII. Conclusion

The shortage of cybersecurity experts, particularly from underrepresented groups, presents a significant barrier to effectively countering cyber threats. By integrating broader concepts such as data sharing, privacy, and ethics, and developing engaging capture-the-flag exercises, it becomes possible to engage a diverse range of learners with varying educational backgrounds. Additionally, there is an urgent need to equip young people with essential digital skills and awareness to navigate the evolving digital landscape.

The research presented in this article is centered around engaging a diverse audience in cybersecurity with the development and testing of Peacock, a social-media-like platform featuring capture-the-flag exercises designed to introduce students to privacy and OSINT concepts in a user-friendly manner. The Peacock CTF exercises effectively introduced high school students to privacy, data sharing, and ethics in cybersecurity. The platform's incorporation of broader concepts enhanced students' interest improved digital literacy, and heightened awareness about cybersecurity. By engaging a diverse group of students, including those without technical backgrounds, we fostered inclusivity and empowered individuals to pursue careers in cybersecurity. The Peacock platform serves as a demonstration of the effectiveness of incorporating diverse educational backgrounds in cybersecurity education, providing a valuable tool for enhancing awareness and improving digital skills, as well as attracting and training a more diverse workforce.

Furthermore, the Peacock platform serves as an idea that can be generalized and adapted according to specific needs, demonstrating its potential to attract and train a more diverse cybersecurity workforce. The findings of this study have broader implications and can be applied to cybersecurity education efforts aimed at bridging the skills gap and promoting diversity in the field.

Credits Author Statement

Mubashrah Saddiqa: Conceptualization, data collection, analysis, writing and finalizing.

Kristian Helmer Kjær Larsen: Conceptualization, workshop design and execution, exercise development, writing.

Robert Nedergaard Nielsen: Conceptualization, workshop design and execution, exercise development, editing and review.

Jens Myrup Pedersen: Conceptualization, editing and review, supervision.

Acknowledgment

We acknowledged Linda Mostrup Pedersen for workshops coordination, Arianna Sammarchi for data collection, the teachers for their insightful feedback, and Industriens Fond for the financial support.

References

[1] (ISC)2, 2021 CYBERSECURITY WORKFORCE STUDY, “A Resilient Cybersecurity Profession Charts the Path Forward”, 2021. https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2021.pdf?rev=5ede8b928b3d43888fae31cf4424265e

[2] (ISC)2, CYBERSECURITY WORKFORCE STUDY, “A critical need for cybersecurity professionals persists amidst a year of cultural and workplace evolution”, 2022. https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx

[3] X. Mountrouidou, D. Vosen, C. Kari, M. Q. Azhar, S. Bhatia, G. Gagne, et al., "Securing the human: a review of literature on broadening diversity in cybersecurity education," Proceedings of the Working Group Reports on Innovation and Technology in Computer Science Education, 2019, pp. 157-176. https://doi.org/10.1145/3344429.3372507

[4] D. N. Burrell, "An exploration of the cybersecurity workforce shortage," in Cyber warfare and terrorism: Concepts, methodologies, tools, and applications, IGI Global, 2020, pp. 1072-1081. DOI: 10.4018/978-1-7998-2466-4.ch063

[5] T. Benzel, "Cybersecurity research for the future," Communications of the ACM, vol. 64, no. 1, 2020, pp. 26-28. https://doi.org/10.1145/3436241

[6] T. Stevens, "Global cybersecurity: New directions in theory and methods," Politics and Governance, vol. 6, no. 2, 2018, pp. 1-4. DOI: 10.17645/pag.v6i2.1569

[7] C. M. Graham and Y. Lu, "Skills expectations in cybersecurity: semantic network analysis of job advertisements," Journal of Computer Information Systems, vol. 63, no. 4, 2023, pp. 937-949. https://doi.org/10.1080/08874417.2022.2115954

[8] I. Hamburg, "SUPPORTING INTERDISCIPLINARITY, DIVERSITY AND INCLUSION IN CYBERSECURITY," in INTED2023 Proceedings, IATED, 2023, pp. 106-111. DOI: 10.21125/inted.2023.0050

[9] N. Azizi and O. Haass, "Cybersecurity Issues and Challenges," in Handbook of Research on Cybersecurity Issues and Challenges for Business and FinTech Applications, IGI Global, 2023, pp. 21-48. DOI: 10.4018/978-1-6684-5284-4.ch002

[10] I. Bernhard, M. Gustafsson, K. Hedström, J. Seyferin, and E. Whilborg, "A digital society for all?: meanings, practices and policies for digital diversity," in 52nd Hawaii International Conference on System Sciences (HICSS-52), January, Grand Wailea, Maui, 8-11, 2019, pp. 3067-3076.

[11] Y. Taylor and Y. Taylor, "Educational diversity: The subject of difference and different subjects," in Palgrave Macmillan UK, 2012, pp. 1-14.

[12] M. Saddiqa, K. H. Kjær Larsen, R. N. Nielsen, L. T. Sørensen, J. M. Pedersen, "Privacy and Security Training Platform for a Diverse Audience," in Proceedings (Springer Proceedings in Complexity) of the International Conference on Cybersecurity, Situational Awareness and Social Media, Cyber Science 2023, in press. https://link.springer.com/book/9789819969739

[13] G.M. Mennecozzi et al., "Bridging the gap: Adapting a security education platform to a new audience," in 2021 IEEE Global Engineering Education Conference (EDUCON), 2021, pp. 153-159. DOI: 10.1109/EDUCON46332.2021.9453985

[14] Esteban Ortiz-Ospina. "The rise of social media". Published online at OurWorldInData.org. Retrieved from: https://ourworldindata.org/rise-of-social-media, 2019. [Online Resource]

[15] E. Bozzola, G. Spina, R. Agostiniani, S. Barni, R. Russo, E. Scarpato, A. Di Mauro, A. V. Di Stefano, C. Caruso, G. Corsello, and A. Staiano, "The Use of Social Media in Children and Adolescents: Scoping Review on the Potential Risks," Int J Environ Res Public Health, vol. 19, no. 16, 2022, p. 9960. DOI: 10.3390/ijerph19169960

[16] M. Madden, A. Lenhart, S. Cortesi, U. Gasser, M. Duggan, A. Smith, and M. Beaton, "Teens, social media, and privacy," Pew Research Center, vol. 21, no. 1055, 2013, pp. 2-86.

[17] V. I. Marín, J. P. Carpenter, G. Tur, and S. Williamson-Leadley, "Social media and data privacy in education: an international comparative study of perceptions among pre-service teachers," Journal of Computers in Education, 2022, pp. 1-27.
https://doi.org/10.1007/s40692-022-00243-x

[18] T. Romeo, "Microsoft at NICE Conference: Resetting expectations and enabling diversity in the cybersecurity workforce," 2023.
https://www.microsoft.com/en-us/security/blog/2023/06/27/microsoft-at-nice-conference-resetting-expectations-and-enabling-diversity-in-the-future-cybersecurity-workforce/ 2023.

[19] D. M. M. Marinova and S. T. Marinova, "Diversity and Inclusion in Cyber Security Early Careers," in Diversity in Action, 2022, pp. 287-310, Emerald Publishing Limited.
https://doi.org/10.1108/978-1-80117-226-420221015