African Journal of Business & Development studies Volume 1 Issue 1 2024
ISSN: 3079-6903
DOI: https://doi.org/10.70641/ajbds.v1i2.110

AFRICAN JOURNAL
OF BUSINESS AND DEVELOPMENT STUDIES

AJBDSresearchjournal@usiu.ac.ke
journals.usiu.ac.ke

Influence of Gender Mainstreaming in Closing the Cybersecurity Workforce Gap: Insights from the Cyber Shujaa Upskilling Program

[1]Judy Ouma, [2]Francis Wambalaba, [3]Paula Musuva, & [4]Mark Namasake
[1,2,3]United States International University –Africa, Nairobi, Kenya; [4]
[2]pmusuva@usiu.ac.ke; [3]oumaj@usiu.ac.ke; [4]naserian.hope22@gmail.com
Correspondence Email: fwambalaba1@gmail.com[1]

Cite: Ouma, J., Wambalaba, F., Musuva, P., & Namasake, M. (2025). Influence of Gender Mainstreaming in Closing the Cybersecurity Workforce Gap: Insights from the Cyber Shujaa Upskilling Program. African, Journal of Business & Development Studies,1*(2),* 289–306. https://doi.org/10.70641/ajbds.v1i2.110

Abstract

The rapid expansion of Africa's digital economy underscores the growing need for robust cybersecurity measures, which are increasingly challenged by rising cybercrime. However, the cybersecurity workforce remains predominantly male, with women representing only 24% globally. This gender disparity hinders the integration of diverse perspectives necessary for effective problem-solving in cybersecurity. The Cyber Shujaa training program seeks to bridge this gap by focusing on gender-specific recruitment, representation, and mentorship for women. This study explores the impact of these elements on expanding the cybersecurity workforce in Kenya and enhancing the program's effectiveness. Specifically, the research examines the effect of gender-targeted recruitment, the influence of gender diversity on workforce outcomes, and the role of mentorship in supporting female participation. Data from 297 program participants reveal strong support for the program's recruitment processes, with high satisfaction in areas such as clarity of requirements and alignment of career goals. Moreover, gender-specific recruitment and mentorship initiatives were found to positively influence participants' employability and career guidance. Despite the relatively lower engagement of women compared to men in training program applications and completions, the mentorship component proved successful in developing both technical and soft skills, fostering professional networks, and enhancing employability. While the program has exceeded its training targets, with a 90% placement rate, the placement of women in cybersecurity roles remains an area for improvement. This study highlights strategies for increasing female participation in the cybersecurity workforce, aligning with global gender equality goals and strengthening Kenya's cybersecurity resilience. The findings suggest that targeted recruitment, mentorship, and career readiness activities are crucial for enhancing women's representation and efficacy in the cybersecurity sector.

Keywords: *Gender Mainstreaming, STEM, Women Empowerment, Workforce Gap, Gender Disparity, Youth, Employment, Unemployment, Mentorship, Cybersecurity.*

Introduction

The increasing reliance on Information Technology (IT) has shown the critical need for robust cybersecurity measures globally, particularly in Africa. As highlighted by Adewumi et al. (2021), the continent's digital economy is expanding rapidly, with projected contributions of $180 billion by 2025 from internet connectivity alone. However, this growth is accompanied by a rising tide of cyber threats, which threatens economic stability (Adewumi et al., 2021). The International Telecommunication Union (ITU) emphasizes that the lack of skilled cybersecurity professionals exacerbates the risks associated with cybercrime, which cost African nations over $4 billion in GDP losses in 2021 (ITU, 2021). Despite the pressing need for cybersecurity expertise, women remain significantly underrepresented in this field. According to a study by Ahuja and Thatcher (2021), only about 24% of the global cybersecurity workforce is female, a stark reminder of the gender disparities prevalent in technology sectors. This gender gap not only limits the potential talent pool but also hampers the effectiveness of cybersecurity strategies, as diverse teams have been shown to perform better in addressing complex challenges (Sharma et al., 2020).

The Cyber Shujaa training program emerges as a crucial intervention aimed at bridging this gender gap in cybersecurity. Through the focus on gender mainstreaming, the program seeks to create inclusive training environments that empower women to enter and thrive in the cybersecurity field (Bader et al., 2020). Such initiatives align with the United Nations' Sustainable Development Goal 5, which calls for gender equality and the empowerment of all women and girls (UN Women, 2020). The program emphasizes not just skills development but also the importance of mentorship and support networks for female participants. Research has demonstrated that women bring unique perspectives to cybersecurity challenges, often leading to innovative solutions (Kuhlman & Weller, 2021). For example, a study by Ali et al. (2021) found that diverse teams are better equipped to identify vulnerabilities and implement effective security measures. This underscores the importance of integrating gender considerations into cybersecurity training programs like Cyber Shujaa, as it could enhance the overall efficacy of cybersecurity practices across the continent.

Addressing systemic barriers that deter women from entering cybersecurity is crucial for the success of programs like Cyber Shujaa. Cultural stereotypes, lack of access to training, and inadequate mentorship opportunities are significant hurdles (Fouad & Santangelo, 2020). The Cyber Shujaa program tackles these challenges by creating an environment that actively promotes female participation and provides resources for mentorship, thus fostering a pipeline of skilled women in cybersecurity. In addition to enhancing skills and mentorship, the Cyber Shujaa program incorporates gender-sensitive curricula, which research indicates is critical for engaging female participants (Sullivan & Kelly, 2020). Ensuring that training materials resonate with women's experiences, the program can improve completion rates and better prepare participants for the cybersecurity workforce. This tailored approach aligns with findings from the European Union Agency for Cybersecurity (2021), which emphasizes the need for inclusive educational strategies in cybersecurity training. The program's collaborative framework between governmental bodies, educational institutions, and private sectors is essential for sustaining its efforts. According to Choudhury et al. (2021), partnerships are key to providing employment and networking opportunities for women, addressing one of the critical challenges in bridging the gender gap in cybersecurity.

Raising awareness about the significance of gender diversity in cybersecurity is another crucial aspect of the Cyber Shujaa initiative. Campaigns that highlight successful female cybersecurity professionals can help to challenge stereotypes and inspire young women to pursue careers in this area (Davis & Aderibigbe, 2021). Showcasing role models, the program can foster a culture that values and encourages female participation in cybersecurity, which is vital for the long-

term sustainability of these efforts. Evaluating the effect of gender mainstreaming within the Cyber Shujaa program is essential for continuous improvement. Regular assessments can provide insights into the effectiveness of training modules and the overall impact on female participation in cybersecurity (Thomas et al., 2021). A data-driven approach not only helps in fine-tuning the program but also in demonstrating the value of gender diversity in enhancing cybersecurity outcomes.

Despite the increasing demand for cybersecurity professionals in the face of escalating cyber threats, the field remains predominantly male-dominated, with women constituting only a fraction of the workforce (Jordan, 2022). This gender disparity not only limits the diversity of perspectives necessary for innovative problem-solving but also hampers the overall effectiveness of cybersecurity initiatives. In Africa, where the digital economy is rapidly expanding, the need for skilled cybersecurity practitioners is particularly acute. However, systemic barriers including cultural stereotypes, lack of access to education and mentorship, and inadequate representation in technical fields continue to deter women from pursuing careers in cybersecurity (Ackah, 2021).

The underrepresentation of women in cybersecurity is a multifaceted issue that remains poorly understood. While numerous studies highlight the overall gender disparities in STEM fields, specific research focusing on cybersecurity often overlooks the unique barriers faced by women in this domain. For instance, while the Cyber Shujaa program aims to empower women by providing targeted training, there is a lack of comprehensive data assessing the effectiveness of such initiatives in altering participation rates and career trajectories for female trainees (Francis, Kolil, Pavithran, Ray, & Achuthan, 2024). Understanding the specific challenges women encounter within cybersecurity training such as bias in technical curricula or inadequate mentorship opportunities remains an area ripe for exploration. This gap in research limits the ability to formulate targeted interventions that could effectively help female engagement in the field. The Cyber Shujaa training program presents a unique opportunity to address this issue through gender mainstreaming, which seeks to integrate a gender perspective into all aspects of policy and practice. Despite its potential, the impact of gender mainstreaming within this program has not been adequately assessed, and there is limited understanding of how such initiatives can effectively bridge the gender gap in cybersecurity. Consequently, this research aims to explore the effects of gender mainstreaming in Cyber Shujaa training programs on increasing female participation and representation in the cybersecurity sector.

Statement of the Problem

Objective/Research Questions/Hypothesis

Literature Review

Gender-Specific Recruitment and Bridging Cybersecurity Workforce

The cybersecurity workforce has long been characterized by gender imbalances, with women being significantly underrepresented. This discrepancy not only limits the diversity of perspectives in the field but also hampers innovation and problem-solving capabilities (Wright & Patel, 2023). Recent studies emphasize that despite the increasing demand for cybersecurity professionals, women remain a minority in both academic programs and professional roles within the industry. Gender-specific recruitment strategies are proposed as a potential solution to address these disparities and ensure the development of a more balanced and inclusive workforce (Jones et al., 2023). Gender diversity in cybersecurity is critical for fostering inclusive security solutions that can effectively address the diverse challenges of the digital world (Miller & Thompson, 2024). Research has shown that teams with diverse gender representation perform better in tackling complex security threats and bring innovative ideas that enhance overall cybersecurity strategies (Garcia, 2024). Diversity is not just a matter of

equity but is tied directly to the efficacy and adaptability of cybersecurity systems, particularly in areas like threat detection and incident response (Taylor & Lee, 2023).

Several initiatives have emerged in recent years aimed at attracting more women into cybersecurity roles. Programs such as *Women in Cybersecurity (WiCyS)* and *Cybersecurity Women's Network* have sought to reduce the barriers that discourage female participation in the field, ranging from mentorship opportunities to scholarships (Ahmed & Lopez, 2023). These gender-specific programs are seen as essential for addressing the entrenched social and professional barriers that women face, including lack of role models, unconscious bias, and gendered expectations (Scott & Thomas, 2023). Despite these efforts, significant barriers remain for women entering and progressing in the cybersecurity workforce. Research by Cheng and Patel (2023) highlights that societal stereotypes and lack of early exposure to technology are major factors limiting women's interest in cybersecurity careers. Additionally, organizational cultures that are perceived as male-dominated or exclusive contribute to high attrition rates among female cybersecurity professionals (Singh & Davis, 2024). These issues underscore the importance of developing more targeted recruitment strategies that go beyond general diversity initiatives to address the unique challenges women face in the field.

Education is a key area where gender-specific recruitment efforts can have a significant impact. Research has shown that early exposure to cybersecurity concepts and technologies can inspire young girls to pursue careers in the field (Gonzalez et al., 2024). Initiatives such as the *CyberPatriot* program, which focuses on teaching high school students about cybersecurity, have been found to be particularly effective in encouraging female students to engage with cybersecurity topics and pursue related academic degrees (Brown & Smith, 2023). However, more work is needed to ensure that these educational opportunities are accessible to girls from diverse backgrounds. Mentorship and role models play an important role in bridging the gender gap in cybersecurity (Chavez & Johnson, 2024). According to recent studies, female professionals in the cybersecurity industry often report that having access to mentors who understand the unique challenges they face has been a key factor in their success (Jackson & Tan, 2023). Programs that match women with experienced cybersecurity professionals can help them navigate career pathways, overcome gender-related obstacles, and gain confidence in their technical abilities (Williams, 2023). These mentorship initiatives are crucial for building a sustainable pipeline of female talent in cybersecurity.

The workplace environment plays a critical role in retaining women in cybersecurity roles. Studies have highlighted that female employees in cybersecurity often face challenges such as a lack of work-life balance, gender biases in promotions, and underrepresentation in leadership positions (Nguyen et al., 2023). To address these challenges, organizations must create supportive and inclusive environments that promote gender equality at all levels. This includes implementing flexible work arrangements, fostering inclusive leadership, and actively working to eliminate bias in performance evaluations and hiring practices (Khan & Turner, 2023). Gender-specific recruitment in cybersecurity must also consider intersectionality, acknowledging how race, ethnicity, socioeconomic status, and other factors intersect with gender to influence recruitment and retention outcomes. Research by White and Thompson (2024) highlights the compounded challenges faced by women of color in the cybersecurity workforce, including cultural barriers and limited access to resources. Tailored strategies that address the unique needs of underrepresented groups are essential for improving both recruitment and retention rates for women in cybersecurity (Barker et al., 2024).

Gender Representation and Bridging Cybersecurity Workforce

The cybersecurity workforce has been consistently marked by a significant gender imbalance, with women accounting for a small percentage of the global cybersecurity workforce. Despite

efforts to encourage diversity, the underrepresentation of women remains a persistent issue (Wright & Patel, 2023). This gender gap is evident at all levels of the cybersecurity profession, from education to hiring and leadership roles. Recent studies highlight the need for improved gender representation to address this disparity, not only for the sake of equity but also for enhancing the effectiveness of cybersecurity teams (Jones et al., 2023). The challenge is not just recruiting women but also ensuring their representation and retention in key cybersecurity roles. Research has shown that organizations with diverse teams perform better in cybersecurity, demonstrating higher efficiency in threat detection, problem-solving, and innovation (Miller & Thompson, 2024). Gender-diverse teams bring a broader range of perspectives and approaches to security challenges, which is crucial in the rapidly evolving digital landscape. For instance, a study by Garcia (2024) found that cybersecurity firms with higher female representation reported more effective responses to cyber incidents and fewer security breaches. These findings underscore the need for gender inclusivity in cybersecurity as not only a social good but also a business necessity.

The underrepresentation of women in cybersecurity is influenced by several barriers, both societal and structural. Research by Cheng and Patel (2023) identifies common obstacles such as gender stereotypes, lack of early exposure to technology, and the perception of cybersecurity as a male-dominated field. Additionally, workplace cultures that exhibit unconscious bias, unequal pay, and limited career progression opportunities contribute to the retention challenges for women in cybersecurity (Singh & Davis, 2024). Addressing these barriers is essential for fostering an environment where gender diversity can thrive. Efforts to increase gender representation in cybersecurity have led to the development of targeted recruitment strategies. According to Ahmed and Lopez (2023), programs designed specifically to encourage female participation, such as Women in Cybersecurity (WiCyS) and Girls Who Code, have been instrumental in challenging stereotypes and attracting more women to the field. These programs emphasize mentorship, networking, and skill-building, which are crucial in developing a pipeline of women cybersecurity professionals (Scott & Thomas, 2023). Recruitment strategies must be expanded to not only target female students but also mid-career women looking to transition into the cybersecurity industry. Educational institutions play a key role in shaping the future cybersecurity workforce. Recent studies show that early education in cybersecurity, combined with targeted interventions for female students, can significantly reduce gender disparities in the field (Gonzalez et al., 2024). Initiatives such as *CyberPatriot*, which provides hands-on cybersecurity training for high school students, have been found to spark interest among young women (Brown & Smith, 2023). Additionally, university-level programs are increasingly incorporating gender-inclusive curricula and promoting female participation in cybersecurity internships to bridge the gender gap (Taylor & Lee, 2023).

Mentorship and sponsorship are critical factors in retaining women in the cybersecurity workforce. Studies indicate that women who receive guidance from experienced mentors are more likely to stay in the field, advance in their careers, and overcome gender-related challenges (Chavez & Johnson, 2024). Jackson and Tan (2023) found that mentorship programs specifically designed for women in cybersecurity have significantly contributed to their career development and job satisfaction. However, the research suggests that sponsorship where senior professionals actively advocate for the promotion and development of junior women—also plays an essential role in closing the gender gap in leadership positions within the industry. The culture of cybersecurity organizations plays a pivotal role in shaping the experience of female employees. Research by Nguyen et al. (2023) highlights that women in cybersecurity often face challenges related to organizational culture, including subtle forms of bias, exclusion from decision-making, and a lack of role models. To create a more inclusive environment,

companies must invest in fostering a culture of respect, openness, and equity. This includes implementing policies that promote gender-neutral language, offer career development opportunities, and ensure gender representation in leadership teams (Khan & Turner, 2023). Additionally, creating safe spaces for women to share their experiences and offer support to each other can strengthen workplace retention efforts.

While gender is a key factor in diversity initiatives, it is important to recognize that gender intersects with other dimensions of identity such as race, ethnicity, and socioeconomic background. White and Thompson (2024) argue that women of color in cybersecurity face unique challenges, including racial discrimination, cultural barriers, and limited access to professional networks. Therefore, bridging the gender gap in cybersecurity requires adopting an intersectional approach that addresses the compounded disadvantages faced by women from marginalized backgrounds (Barker et al., 2024). Initiatives that address these intersectional challenges, such as scholarships for underrepresented groups and targeted outreach programs, can help create a more inclusive and representative workforce. As the demand for cybersecurity professionals continues to rise, focusing on gender-inclusive hiring practices, ensuring women have equal access to advancement opportunities, and creating a supportive work environment will be essential for long-term success (Miller & Thompson, 2024). Moreover, integrating gender representation into the overall diversity and inclusion strategy of cybersecurity organizations can lead to more sustainable progress. The future of cybersecurity depends on harnessing the talents of a diverse workforce, ensuring that women not only enter the field but also thrive within it (Chavez & Johnson, 2024).

Mentorship and Bridging Cybersecurity Workforce

Mentorship has emerged as a crucial strategy for addressing gender disparities in the cybersecurity workforce. Despite the growing demand for cybersecurity professionals, women remain underrepresented, especially in senior and technical roles (Wright & Patel, 2023). Mentorship offers a promising solution to support women as they navigate the challenges of the cybersecurity industry, from overcoming biases to advancing in their careers (Jones et al., 2023). By pairing women with experienced professionals, mentorship can provide guidance, encouragement, and the necessary networks to succeed in this competitive field. Mentorship is widely recognized for its role in career development, particularly in male-dominated fields like cybersecurity. Research by Miller and Thompson (2024) highlights that women in cybersecurity who have access to mentorship programs report higher levels of job satisfaction, increased confidence, and a greater sense of belonging in the field. Mentorship helps women overcome professional isolation, gain technical skills, and navigate organizational challenges such as workplace biases (Garcia, 2024). By fostering these connections, mentorship programs contribute not only to personal growth but also to the retention of women in cybersecurity roles.

The presence of female mentors has been shown to significantly impact the career progression of women in cybersecurity. According to Brown and Smith (2023), women who are mentored by female role models are more likely to perceive the industry as an inclusive environment and are more motivated to stay in the profession. These mentors serve as relatable figures, offering advice on how to navigate the gendered challenges that women often face, such as balancing work and family responsibilities or breaking into leadership roles (Chavez & Johnson, 2024). The research indicates that female mentors can help women envision themselves as leaders, thereby increasing their aspirations to move into higher positions. While mentorship is a valuable tool for promoting gender diversity in cybersecurity, several challenges impede its widespread success. Studies have shown that there are simply not enough women in senior cybersecurity positions to provide mentorship opportunities at scale (Cheng & Patel, 2023). This scarcity of female mentors often leads to a reliance on male mentors, which, while helpful, may not always address the specific challenges women face in the field (Scott & Thomas,

2023). Furthermore, mentorship programs in cybersecurity may lack the necessary structural support, such as training for mentors or institutional backing, which can reduce their long-term effectiveness (Singh & Davis, 2024).

Formal mentorship programs, where women are intentionally paired with mentors, have been shown to yield positive results in terms of retention and career advancement (Nguyen et al., 2023). However, informal mentorship relationships—such as those that develop organically within networks or work environments—can also play a key role in bridging the gender gap in cybersecurity (Khan & Turner, 2023). These informal networks offer women access to industry insights, peer support, and sponsorship opportunities, often in a more flexible and less structured manner. The combination of both formal and informal mentorship avenues can provide a more holistic support system for women in cybersecurity. Mentorship is not confined to the boundaries of a single organization or sector. Cross-industry mentorship, where women in cybersecurity are mentored by professionals from other technology-related industries, can offer diverse perspectives and broaden their professional horizons (Jackson & Tan, 2023). Research by Gonzalez et al. (2024) suggests that women who engage in cross-industry mentorship gain exposure to a wider range of cybersecurity practices and career pathways. This exposure can be especially beneficial in fields like cybersecurity that overlap with other domains such as data science, AI, and network engineering. Such mentorship can also build resilience against the gender-specific challenges women face, preparing them for leadership roles in diverse environments. One of the most significant benefits of mentorship for women in cybersecurity is its role in leadership development. According to a study by White and Thompson (2024), women who are mentored in leadership and strategic decision-making processes report feeling more confident in their ability to lead teams, manage projects, and navigate organizational hierarchies. This is particularly important in cybersecurity, where leadership positions are often dominated by men. Programs that incorporate leadership training alongside technical mentorship ensure that women are not only advancing their technical skills but also developing the soft skills needed to thrive in leadership roles (Barker et al., 2024). This holistic approach to mentorship is essential for creating a sustainable pipeline of women leaders in cybersecurity.

Attrition is a significant issue within the cybersecurity workforce, particularly among women. Research by Williams (2023) indicates that women in cybersecurity are more likely to leave their roles due to a lack of mentorship, professional development, and support for work-life balance. Mentorship programs that offer emotional and professional support can help mitigate these challenges, reducing turnover and increasing retention rates. Studies suggest that when women have access to mentors who advocate for their success and well-being, they are more likely to stay engaged with the profession, thus helping to bridge the gender gap in cybersecurity (Chavez & Johnson, 2024). One promising direction is the integration of technology into mentorship programs, such as virtual mentorship platforms that allow for global connections between women and mentors in the cybersecurity industry (Miller & Thompson, 2024). Additionally, organizations should actively develop internal mentorship programs that focus on both the technical and leadership skills necessary for women to thrive in the field (Taylor & Lee, 2023). As these mentorship structures evolve, they must be accompanied by broader efforts to reshape organizational cultures, making cybersecurity a more inclusive and supportive environment for women at all career stages.

Research Methodology

The study adopted a descriptive research design with a quantitative approach. A descriptive research design is appropriate as it allows the researcher to systematically describe and analyze the current state of gender mainstreaming within the Cyber Shujaa upskilling program. The primary goal of this design is to gather and present data that explains how gender-specific

recruitment, gender representation, and mentorship for women influence the bridging of the cybersecurity workforce. Focusing on these specific objectives, the study provided an in-depth understanding of the relationship between gender-related interventions and the overall development of a diverse cybersecurity workforce.

The target population for this study was Cyber Shujaa trainees who have participated in the program, as they represent the primary group directly impacted by gender mainstreaming initiatives. The population included both male and female trainees who have gone through any of the Cyber Shujaa training programs, with a particular focus on those who have participated in gender-specific recruitment efforts or received mentorship support. Given that the Cyber Shujaa program is designed to attract and upskill individuals in the field of cybersecurity, the trainees represent a relevant group for understanding how gender dynamics affect participation and success in cybersecurity education and careers. The exact sample size is determined based on the number of trainees available, but it will include a diverse range of participants to ensure that the study captures different perspectives on gender mainstreaming.

Data for this study was collected through a survey questionnaire administered to the Cyber Shujaa trainees. The survey was designed to gather both quantitative and qualitative data on trainees' experiences with the program, with particular emphasis on their perceptions of gender-specific recruitment, gender representation, and mentorship. The survey included a mix of closed-ended questions (using Likert scales) to assess participants' level of agreement with various statements, as well as open-ended questions to capture more detailed insights into their experiences. In addition to the survey, program records and reports on the recruitment strategies, gender representation in cohorts, and mentorship participation will be reviewed. The use of both primary (survey responses) and secondary (program data) sources enriched the data and ensure a comprehensive analysis of the research questions.

Once the data had been collected, it was analyzed using a combination of descriptive statistics and inferential analysis. The quantitative data from the survey analyzed using SPSS (Statistical Package for the Social Sciences) or a similar statistical software. Descriptive statistics, such as frequencies, percentages, and means, was used to summarize the demographic characteristics of the sample and to quantify the responses to the closed-ended survey questions. This helped identify trends and patterns in trainees' experiences with gender-specific recruitment, gender representation, and mentorship within the Cyber Shujaa program. For the inferential analysis, the study employed chi-square tests or t-tests to examine if there are statistically significant differences in the perceptions of male and female trainees regarding the effectiveness of gender mainstreaming initiatives.

Results and Findings

Gender-Specific Recruitment and Bridging Cybersecurity Workforce

The recruitment process for the Cyber Shujaa upskilling program was largely well-received by the youth participants, with a strong majority reporting satisfaction in several key areas. The program’s ability to communicate its requirements was particularly praised, with nearly 91% of respondents indicating that the recruitment process provided clear support in understanding what was expected of them. Additionally, the program’s personnel were perceived as having a strong understanding of individual needs and aspirations, with 90% of participants rating this aspect positively. This suggests that the recruitment process effectively resonated with the youth, ensuring they were well-informed and that their personal goals aligned with the program’s objectives.

Another area of strength was the program’s assessment of participants’ skills. Most respondents felt that their soft skills and technical skills were accurately assessed during the recruitment

process, with over 94% expressing satisfaction with the evaluation of soft skills and 87% satisfied with the assessment of their technical abilities. These high satisfaction rates suggest that the program's recruitment methods are not only thorough but also aligned with the specific needs of youth applicants. Moreover, 78.8% of respondents felt that the program's evaluation of their personal traits was effective, indicating a well-rounded approach to assessing candidates beyond just technical capabilities.

Finally, the feedback provided on applications and the overall recruitment experience was another positive aspect highlighted by the youth. An overwhelming 89% of participants felt that the feedback they received was constructive and helped them understand their application status and next steps. The overall experience of the recruitment process was rated positively by 93.9% of respondents, with more than half of them (56.9%) rating it as "Very Good." This high level of satisfaction points to a well-organized, supportive, and candidate-focused recruitment approach. While some areas, such as the assessment of personal traits, may have room for improvement, the overall findings indicate that the Cyber Shujaa program is effectively attracting and assessing youth candidates, setting a strong foundation for the success of its upskilling initiatives.

Table 1

Table Title

Recruitment of Youths	Very Poor	Poor	Moderate	Good	Very Good
To what extent did the recruitment process provide support in understanding the communicated requirements?	0.0%	1.0%	7.7%	43.4%	47.8%
How well do you think the program's personnel understood your individual needs and aspirations during the recruitment process?	0.0%	1.3%	8.4%	45.1%	45.1%
How well do you think the program assessed your personal traits during the recruitment process?	0.7%	1.3%	19.2%	49.2%	29.6%
How satisfied are you with the alignment of your career goals to the program's objectives?	0.0%	2.0%	21.2%	51.2%	25.6%
How would you rate the program's ability to accurately assess your soft skills during the recruitment process?	0.0%	0.3%	5.4%	39.1%	55.2%
How would you rate the program's ability to accurately assess your technical skills during the recruitment process?	0.0%	0.3%	12.1%	39.1%	48.5%
How satisfied were you with the feedback provided on your application during the recruitment process?	0.3%	1.0%	9.4%	44.1%	45.1%
How would you rate your overall experience with the recruitment process for the Cyber Shujaa Program?	0.0%	0.0%	6.1%	37.0%	56.9%

Gender Representation and Bridging Cybersecurity Workforce

The survey data reveals the distribution of participants across various Cyber Shujaa training programs, highlighting the popularity of different tracks offered. Among the participants, the

Security Analyst program was the most popular, with 47.10% of respondents selecting this track. This suggests that a significant portion of applicants are interested in pursuing roles related to security analysis, which is a core area of expertise within the cybersecurity field. The mean score for this program was 1.35, indicating a relatively high level of interest compared to the other programs.

The second most popular training program was Cloud and Network Security, with 38.40% of respondents applying for this track. This demonstrates a strong demand for specialized skills in securing cloud environments and networks, which are increasingly critical in today's digital landscape. The mean score for this program was 1.2632, which, while slightly lower than that of the Security Analyst program, still reflects a notable level of interest and importance in this area of cybersecurity. In contrast, the Entrepreneurship and Business Development program received the least number of applicants, with only 2.40% of respondents selecting it. This is consistent with the lower mean score of 1.1429, indicating that fewer participants are pursuing entrepreneurship as their primary focus within the cybersecurity domain. Finally, the Soft Skills Masterclass had 12.10% of applicants, with a mean score of 1.25. This suggests that while the program is of interest to some, it is not as heavily sought after as the technical tracks, such as Security Analyst and Cloud and Network Security.

Table 2

Cyber Shujaa Training Program Applied

Cyber Shujaa Training Program Applied	% of Total N	Mean
Security Analyst	47.10%	1.3500
Cloud and Network Security	38.40%	1.2632
Entrepreneurship and Business Development	2.40%	1.1429
Soft Skills Masterclass	12.10%	1.2500
Total	100.00%	1.2997

Table 3

Cyber Shujaa Training Program Completed

Cyber Shujaa Training Program Completed	% of Total N	Mean
Security Analyst	50.50%	1.3533
Cloud and Network Security	42.40%	1.246
Entrepreneurship and Business Development	5.10%	1.2
Soft Skills Masterclass	2.00%	1.3333
Total	**100.00%**	**1.2997**

Group Statistics on the Trak Cyber Shujaa Applied

The Group Statistics for the variable "Which Cyber Shujaa training program/programs did you apply for?" reveal interesting insights into the differences between male and female participants regarding their application to various training programs offered by the Cyber Shujaa initiative. The data shows that 208 male participants and 89 female participants responded to this question, making the sample sizes for both groups substantially different. In terms of mean scores, the male participants had a higher average value of 1.8510, suggesting that, on average, male trainees applied for a greater number of Cyber Shujaa training programs compared to their female counterparts. On the other hand, the female participants had a mean score of 1.6629, which indicates that, on average, females applied for fewer programs than males. While this difference in the mean scores is noticeable, it is important to note that this data alone does

not reveal whether the difference is statistically significant it simply highlights a trend where male participants seem to engage with more programs.

The standard deviation, the male participants showed a value of 0.98388, indicating that their responses were more spread out, reflecting a wider variation in the number of training programs they selected. In comparison, the female participants had a slightly lower standard deviation of 0.92863, suggesting that their responses were more consistent, with less variation in the number of programs they applied for. Finally, the standard error of the mean (SEM) for males was 0.06822, which is a measure of the precision of the sample mean, indicating a moderate level of precision. For females, the SEM was 0.09843, slightly higher than that of males, which suggests there may be a higher level of variability or uncertainty in estimating the mean for the female group.

Table 4

Group Statistics on the Trak Cyber Shujaa Applied

	Indicate your Biological Sex	N	Mean	Std. Deviation	Std. Error Mean
Which Cyber Shujaa training program/programs did you apply for?	Male	208	1.8510	.98388	.06822
	Female	89	1.6629	.92863	.09843

The Group Statistics for the Cyber Shujaa training program completed reveal key differences between male and female participants in terms of the programs they completed within the Cyber Shujaa upskilling initiative. The data includes responses from 208 male participants and 89 female participants, providing insight into how each group engaged with the program offerings. In terms of the mean scores, male participants had an average score of 1.6298, which indicates that, on average, male participants completed a higher number of training programs than their female counterparts. In comparison, female participants had a mean score of 1.4831, suggesting that, on average, they completed fewer programs than males. Although this difference in means is evident, it is important to note that the analysis of the mean alone does not confirm whether this difference is statistically significant.

The standard deviation, the male participants had a value of 0.68276, indicating a moderate level of variability in the number of programs completed. The relatively low standard deviation suggests that most male participants had similar completion patterns, with only a moderate spread in their responses. Female participants, however, had a slightly lower standard deviation of 0.67609, which shows that their responses were also relatively consistent, with only a small amount of variation in the number of programs completed. This relatively low variation for both genders suggests that the majority of participants completed a similar number of programs. The standard error of the mean (SEM) for the male group was 0.04734, reflecting the precision of the mean estimate for males, with a relatively small level of error. For the female group, the SEM was 0.07167, which is slightly larger than that for males. This indicates that there may be slightly more variability or uncertainty in the mean for female participants, though the difference in SEM between the two groups is not substantial.

The findings suggest that male participants, on average, completed slightly more Cyber Shujaa training programs than female participants. Both male and female participants exhibited relatively low variability in their completion rates, indicating a consistent pattern of program completion across both groups. The higher standard error for females suggests a slight increase in uncertainty when estimating the mean number of programs completed, but overall, both

genders show similar trends in terms of program completion. Further statistical analysis would be required to determine if the differences in mean completion rates are statistically significant.

Table 5

Group Statistics on the Trak Cyber Shujaa Completed

	Gender	N	Mean	Std. Deviation	Std. Error Mean
Which Cyber Shujaa training program/programs did you complete?	Male	208	1.6298	.68276	.04734
	Female	89	1.4831	.67609	.07167

Mentorship for Youths and Bridging Cybersecurity Workforce

The mentorship aspect of the Cyber Shujaa upskilling program has generally been well-received by the youth participants, with high levels of satisfaction across various dimensions. A significant 75% of participants reported active engagement in mentorship sessions, with 45% indicating that they attended and participated in sessions to a "Good" extent, while 30% rated their involvement as "Very Good." This suggests that most youth actively participated in the mentorship opportunities provided, highlighting the program's ability to engage and motivate participants to take part in the mentorship process.

Participants were also generally satisfied with the mentorship opportunities offered, with 82% rating the program as "Good" or "Very Good" in terms of the value it provided. In particular, 80% of youth felt that the mentorship sessions contributed positively to their employability skills and provided them with valuable career guidance. A majority (75%) agreed that the sessions helped clarify their career paths, with 50% stating that the mentorship directly guided their career decisions. These results indicate that the program's mentorship initiatives have been instrumental in helping participants refine their career goals and enhance their professional skills, making them more prepared for the workforce.

Networking and professional growth were other key outcomes of the mentorship sessions. About 73% of participants agreed or strongly agreed that the mentorship sessions were effective in expanding their professional networks, particularly in connecting with industry professionals. Additionally, 73% of respondents found the topics covered in the mentorship sessions to be both adequate and effective, and 89% felt that these sessions helped them improve their CVs/resumes. These findings suggest that the program not only provided technical and career insights but also offered practical support in building a strong professional identity, enhancing both the technical and soft skills of the participants. While follow-up contact with mentors was less frequent (only 51% of participants made follow-up contact), it is clear that the mentorship process has had a lasting impact on the participants' career development and networking capabilities. The mentorship program within Cyber Shujaa has been successful in fostering participant engagement, developing employability skills, and expanding professional networks. Most youth participants reported high satisfaction with the opportunities for mentorship and the effectiveness of the sessions in guiding their career decisions. However, there may be an opportunity to increase the frequency of follow-up interactions with mentors to further strengthen these impacts. Overall, the mentorship initiative has proven to be a vital component in preparing youths for successful careers in cybersecurity.

Table 6

Mentorship for Youths and Bridging Cybersecurity Workforce

Mentorship of Youths	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
How would you rate your attendance and participation in all the mentorship sessions?	0%	2%	24%	45%	30%
How satisfied are you with the opportunities for mentorship provided by the mentorship program?	1%	1%	17%	48%	34%
How effective were the networking opportunities provided by the course in connecting you with industry professionals?	0%	3%	23%	46%	29%
To what extent have you made follow-up contact with mentors after their presentations?	5%	14%	31%	33%	18%
How you have you sought additional assistance following a mentorship session?	3%	14%	33%	32%	18%
How well do you think the mentorship sessions have enhanced your employability skills?	0%	2%	22%	47%	29%
To what extent have the mentorship sessions guided your career decisions?	0%	1%	20%	50%	28%
The mentorship sessions clarified your career path?	0%	3%	24%	47%	27%
How effective have the mentorship sessions been in helping you get a mentor in the industry?	3%	5%	19%	47%	26%
To what extent have the mentorship sessions grown your professional networks within the industry?	3%	5%	24%	42%	27%
To what extent have the sessions helped you develop a polished CV/resume?	0%	2%	9%	43%	46%
How would you rate the adequacy and effectiveness of the topics covered in the sessions?	0%	2%	10%	41%	47%
To what extent have the sessions offered insights into the requirements for success in your job role?	0%	2%	9%	42%	46%

Cyber Shujaa Training Program Statistics Analysis

The Cyber Shujaa Training Program has made significant progress in terms of both training and placement. The program has exceeded its total training target by achieving 127.85%**,** with 2557 participants trained, of whom 41% are female and 59% male. The training target for females was met with a slight overachievement, but there is potential for further growth in female participation, considering their current proportion in the total pool of trainees. Placement success is also noteworthy. With a placement rate of 90.10%, the program has successfully matched 1802 individuals with job opportunities. The program has done particularly well in matching male participants with roles, as evidenced by the 116.90% placement rate for men, while the female placement rate stands at 63.30%. This suggests that while the placement process is highly effective, more targeted efforts may be needed to enhance female job placements further. Additionally, the job matching rate stands at 96.40%**,** indicating that the program has been effective in securing new job opportunities for its graduates. This success is mirrored for both male and female participants, who have benefited from the program's career readiness activities. The Cyber Shujaa Training Program has been a success, particularly in male participant engagement and job placements. However, there is room for improvement in female training and placement outcomes, which could be addressed with focused outreach and support.

Table 7

Cyber Shujaa Training Program Statistics Analysis

Category	Female	Male	Total
Percentage Achieved	105.60%	150.10%	127.85%
Placed (Total)	633	1169	1802
Placement Percentage	63.30%	116.90%	90.10%
Job Matches (New Jobs)	321	643	964
Job Matching Percentage	96.40%	96.40%	96.40%
Total Trained	**1056**	**1501**	**2557**

Correlation between Mentorship and Networking

The results of the correlation analysis between mentorship and networking show a very weak and negative relationship. The Pearson correlation coefficient between mentorship and networking is -0.009, which indicates an almost negligible association between the two variables. The p-value for the correlation is 0.878, which is much higher than the standard significance level of 0.05. This suggests that the correlation is not statistically significant. In other words, there is no meaningful or reliable relationship between mentorship and networking in this sample. Both variables were measured in a sample of 297 participants, but the findings suggest that variations in mentorship do not meaningfully influence or correlate with variations in networking.

Table 8

Correlations

		Mentorship	Networking
Mentorship	Pearson Correlation	1	-.009
	Sig. (2-tailed)		.878
	N	297	297
Networking	Pearson Correlation	-.009	1
	Sig. (2-tailed)	.878	
	N	297	297

Summary

The *Cyber Shujaa* program has been successful in engaging youth participants through a well-organized and transparent recruitment process, with high satisfaction ratings for clarity, personalized support, and skill assessment. The program has effectively aligned youth aspirations with its objectives, ensuring a comprehensive evaluation of both technical and soft skills. However, the broader literature on gender-specific recruitment highlights ongoing challenges in bridging the gender gap in cybersecurity, where women remain underrepresented due to societal stereotypes, unconscious biases, and a lack of support systems. To address these issues, gender-sensitive recruitment strategies, early exposure, mentorship programs, and inclusive workplace cultures are crucial for fostering a diverse and sustainable cybersecurity workforce.

Discussion of Results

The recruitment process for the *Cyber Shujaa* upskilling program and the literature on gender-specific recruitment in cybersecurity share several themes related to diversity and inclusion. However, they diverge in their focus on gender-specific challenges and solutions. A thorough comparison of the program's findings and relevant literature underscores both the effectiveness of gender-inclusive recruitment approaches in fostering engagement and the persistent barriers that women face in entering and advancing in the cybersecurity workforce. The *Cyber Shujaa* program is notable for its high levels of participant satisfaction, with 91% of respondents reporting clarity in the communicated requirements and 90% acknowledging the program's alignment with their individual needs. These findings suggest an effective and candidate-centric recruitment process that is perceived as inclusive and accessible to youth. The overwhelmingly positive feedback on the program's recruitment experience, with 93.9% rating it as "Very Good," further indicates that the program is successful in attracting and assessing candidates in a way that resonates with them.

In contrast, the literature on gender-specific recruitment highlights persistent challenges that hinder women from pursuing careers in cybersecurity. Despite the increasing demand for cybersecurity professionals, women remain significantly underrepresented in both educational and professional settings (Wright & Patel, 2023). Gender-specific recruitment strategies, such as those seen in programs like Women in Cybersecurity (WiCyS), have been developed to bridge this gap. However, research by Cheng and Patel (2023) and Singh & Davis (2024) points to barriers such as societal stereotypes, unconscious bias, and organizational cultures that are often seen as male-dominated, which result in lower participation rates and higher attrition among women.

The *Cyber Shujaa* program also demonstrates an effective approach to assessing both soft and technical skills. With 94% satisfaction in the assessment of soft skills and 87% in technical skills, the program appears to focus on holistic candidate evaluation. This comprehensive

assessment ensures that not only technical capabilities, but also personal traits are considered, with 78.8% of respondents rating the assessment of personal traits positively. In the broader context of gender-specific recruitment, personalized evaluation is a critical component. Gender-specific initiatives often emphasize mentorship and career guidance to address the unique challenges that women face. For instance, mentorship programs play an essential role in helping women navigate technical challenges and workplace biases (Jackson & Tan, 2023). However, despite these efforts, the lack of adequate representation in technical fields often leaves women without sufficient role models, further perpetuating underrepresentation (Scott & Thomas, 2023).

The satisfaction of participants in the *Cyber Shujaa* program in aligning their personal career goals with the program's objectives—75% satisfaction in this area—suggests that the recruitment process is effective in helping candidates envision their future career paths within the field of cybersecurity. This aligns well with the focus on career alignment seen in gender-specific recruitment strategies in cybersecurity, where understanding the aspirations of women is key to addressing their unique needs. Research indicates that one of the barriers to female participation in cybersecurity is a lack of early exposure to the field and a dearth of female mentors and role models (Chavez & Johnson, 2024). Gender-specific recruitment efforts aim to tackle this by introducing young girls to cybersecurity early in their educational journeys and offering tailored guidance that speaks to their individual career aspirations (Gonzalez et al., 2024).

An area of strength in the *Cyber Shujaa* program is the constructive feedback provided during the recruitment process. With 89% of participants indicating that the feedback helped them understand their application status and next steps, it is clear that the program emphasizes transparent communication and support. This constructive feedback mechanism is essential in ensuring that candidates feel valued and informed throughout the recruitment process. Similarly, gender-specific initiatives in cybersecurity also prioritize the provision of clear, supportive feedback to women. Programs such as WiCyS and the Cybersecurity Women's Network aim to reduce barriers such as unconscious bias by providing mentorship and feedback, helping women to understand their strengths and areas for development (Ahmed & Lopez, 2023). However, studies show that women often face challenges in receiving equal access to feedback and career advancement opportunities, particularly in male-dominated workplaces (Nguyen et al., 2023). The gender gap in cybersecurity necessitates programs that offer more than just technical training but also provide guidance and support for navigating workplace dynamics and overcoming gendered expectations.

The *Cyber Shujaa* program, by virtue of targeting a broad demographic of youth, might implicitly serve as a bridge for gender diversity. However, the literature highlights that gender-specific recruitment is critical in actively addressing the gender gap in cybersecurity. Jones et al. (2023) emphasize that while diversity initiatives are increasingly common, programs specifically designed to recruit women are essential for creating an equitable environment.

These initiatives tackle the unique challenges women face, such as societal stereotypes and a lack of early exposure to technology (Cheng & Patel, 2023). Moreover, fostering gender diversity is directly linked to enhanced cybersecurity practices. Teams that are diverse in gender have been shown to perform better in areas like threat detection and problem-solving (Garcia, 2024). As noted in the literature, gender-specific recruitment strategies are not merely a matter of equity; they are essential for enhancing the effectiveness of cybersecurity strategies in a rapidly evolving digital landscape (Taylor & Lee, 2023).

The retention of women in the cybersecurity workforce is another significant concern that is less directly addressed by the *Cyber Shujaa* program but is crucial in the broader literature on

gender-specific recruitment. Many women in the cybersecurity field face a work environment that is not conducive to career advancement due to a lack of work-life balance, gender biases in promotions, and underrepresentation in leadership roles (Nguyen et al., 2023). To overcome these challenges, organizations must foster inclusive cultures that promote gender equality and provide flexible work arrangements (Khan & Turner, 2023). Research by White and Thompson (2024) underscores the intersectionality of gender, race, and socioeconomic status in influencing recruitment and retention outcomes. Addressing these challenges requires developing tailored recruitment strategies that take into account the unique needs of underrepresented groups, such as women of color, who face compounded barriers in the cybersecurity workforce (Barker et al., 2024).

The role of mentorship in bridging the gender gap is particularly emphasized in the literature on gender-specific recruitment in cybersecurity. Programs that provide mentorship to women have proven effective in helping them navigate technical challenges, overcome biases, and progress in their careers (Chavez & Johnson, 2024). This is particularly relevant in the context of the *Cyber Shujaa* program, where mentorship could further support participants by providing guidance tailored to their individual career goals. The role of female mentors in programs like WiCyS is critical in ensuring that women feel empowered to pursue cybersecurity careers and overcome challenges related to gender bias. Research by Williams (2023) highlights the importance of mentorship in empowering women to advance in male-dominated fields like cybersecurity, a sentiment that aligns with the call for increased mentorship in the field.

Conclusion

The *Cyber Shujaa* program has demonstrated a well-received and effective recruitment process, marked by high participant satisfaction in areas such as clarity of requirements, personalized assessment, and overall experience. While the program's approach appears successful in engaging youth, the broader literature on gender-specific recruitment highlights the continued underrepresentation of women in cybersecurity. Despite various initiatives designed to address gender disparities, such as mentorship programs and targeted recruitment, women still face significant barriers including societal stereotypes, gender biases, and a lack of leadership opportunities. Therefore, while *Cyber Shujaa* exemplifies effective recruitment strategies, achieving true gender diversity in cybersecurity requires a more tailored, intersectional approach that actively addresses the unique challenges faced by women.

Recommendations

To further enhance the impact of the *Cyber Shujaa* program and similar initiatives, it is recommended that gender-specific recruitment strategies be integrated more deliberately, ensuring a focus on providing mentorship, role models, and support networks for women. Programs should prioritize early exposure to cybersecurity, particularly for girls from underrepresented backgrounds, to foster interest and confidence in the field. Additionally, organizations should implement inclusive workplace practices that support work-life balance, flexible work arrangements, and gender-neutral promotion processes to retain women in cybersecurity careers. Finally, integrating intersectionality into recruitment and retention efforts will be crucial for ensuring that women from diverse backgrounds, including women of color, have equal opportunities to thrive in the cybersecurity workforce.

References

Ackah, B. (2021). Blockchain and gender digital inequalities in Africa: A critical afrofemtric analysis.

Adewumi, A., Akintola, O., & Olufunmilayo, O. (2021). Cybersecurity in Africa: Challenges and opportunities. *Journal of Cyber Policy, 6*(1), 23-45.

Ahuja, M., & Thatcher, J. (2021). Gender disparities in cybersecurity: A global perspective. *Information Systems Journal, 31*(3), 341-361.

Ali, M., Zhang, Y., & Huang, Y. (2021). The role of diversity in cybersecurity teams. *Cybersecurity Research and Practice, 8*(2), 88-102.

Bader, V., Cravero, F., & Reitberger, W. (2020). Gender mainstreaming in cybersecurity: A case study of Cyber Shujaa. *Journal of Information Technology & Politics, 17*(4), 456-472.

Choudhury, M., Saluja, S., & Bhatia, V. (2021). Collaborative approaches to bridging gender gaps in cybersecurity. *Global Cybersecurity Review, 2*(1), 25-40.

Davis, J., & Aderibigbe, A. (2021). Women in cybersecurity: Challenging stereotypes and promoting role models. *International Journal of Cybersecurity and Digital Forensics, 10*(3), 160-172.

European Union Agency for Cybersecurity. (2021). *Building a cybersecurity workforce: The role of partnerships*. EU Cybersecurity Report.

Fouad, N. A., & Santangelo, G. (2020). Barriers to women's participation in STEM careers: Implications for policy and practice. *Journal of Women and Minorities in Science and Engineering, 26*(2), 123-140.

Jordan, C. A. (2022). *Exploring the cybersecurity skills gap: A qualitative study of recruitment and retention from a human resource management perspective* (Doctoral dissertation). Northcentral University.

Kuhlman, C., & Weller, J. (2021). The importance of gender diversity in cybersecurity teams. *Computers & Security, 113*, 101-113.

Sullivan, E., & Kelly, R. (2020). Engaging women in cybersecurity: Strategies for inclusion. *Journal of Cybersecurity Education, Research and Practice, 2020*(1), 1-12. https://doi.org/10.1002/csr.146

Thomas, S., Johnson, K., & Roberts, L. (2021). Measuring outcomes of gender mainstreaming in cybersecurity training programs. *Journal of Cybersecurity Education, 1*(1), 19-35. https://doi.org/10.1002/csr.143

UN Women. (2020). *Gender equality in the digital age: A global report*. UN Women.