sciendo

Scientific Bulletin
Vol. XXVIII, No. 2(56), 2023

ADDRESSING BIO-CYBERSECURITY WORKFORCE EMPLOYEE SHORTAGES IN BIOTECHNOLOGY AND HEALTH SCIENCE SECTORS IN THE U.S.

Darrell Norman BURRELL
dburrell2@thechicagoschool.edu

Ian MCANDREW
irmcandrew@captechu.edu

CAPITOL TECHNOLOGY UNIVERSITY, LAUREL MARYLAND, USA

ABSTRACT:

The ever-increasing demand for employees with cybersecurity and artificial intelligence expertise in healthcare technology roles has resulted in an unprecedented skills shortage. Historically Black Colleges and Universities (HBCUs) and Historically Women's Colleges (HWCs) can significantly develop under-represented and diverse talent in this field. As bio-cybersecurity concerns widen, there is an urgent need for individuals with skillsets related to the security of biological payloads and systems. In addition, the inclusion of traditionally under-represented groups into the cybersecurity workforce is necessary to ensure the diversity of skills and security knowledge needed to combat cyberattacks. This paper will discuss how HBCUs and HWCs can contribute to diversifying the cybersecurity workforce, their role in developing artificial intelligence (AI) and bio-cybersecurity talent, and how they can provide an educational platform for new and under-represented talent in the field. It will also address the need for experienced artificial intelligence experts, bio-cybersecurity professionals, educators, and policymakers to facilitate the integration of cybersecurity experts into the traditional biological workforce. Ultimately, this paper will demonstrate how the inclusion of diverse and traditionally under-represented individuals in bio-cybersecurity and artificial intelligence (AI) will benefit the security infrastructure of biological systems.

KEYWORDS:

Artificial intelligence, bio-cybersecurity, Historically Black Colleges and Universities (HBCUs), Historically Women's Colleges (HWCs), cybersecurity workforce development, biotechnology, healthcare cybersecurity

1. Introduction

Artificial Intelligence (AI) has ushered in a new era of technological advancement with transformative potential across multiple domains. While the positive contributions of AI to healthcare, industry, and research are well-documented, it also presents unique challenges, particularly in the realm of bio-cybersecurity and biotechnology. The intersection of AI, bio-cybersecurity, and biotechnology with a particular focus on the potential risks associated with AI-enabled

DOI: 10.2478/bsaft-2023-0014
© 2023 Darrell Norman Burrell et al. This work is licensed under the Creative Commons Attribution-Non Commercial-No Derivatives 3.0 License.

activities that could inadvertently or intentionally lead to the development of novel pathogens, viruses, bioweapons, or chemical weapons. Such endeavors pose significant global biological catastrophic risks, threatening life, national governments, international relationships, economies, societal stability, and global security (Mandile, 2022; Potter, Mossburg & Palmer, 2023).

Bio-cybersecurity is the study of cybersecurity and artificial intelligence in the health sciences, biotechnology, and biological realms; that is, the science of protecting biological systems such as human cells, plants, and animals from malicious invasion and exploitation through cyber threats. Over the past decade, the use of automated cyber-based tools to manipulate and exploit life forms has become increasingly prevalent, raising significant concerns about the safety of our biological systems (Millett et al., 2019; Palmer et al., 2021). Understanding the risks and potential solutions of bio-cybersecurity is essential to protecting our world's biological systems and maintaining a healthy ecosystem.

AI technologies have exhibited tremendous promise in advancing scientific research, healthcare diagnostics, and disease prediction. However, the same AI capabilities that drive innovation also introduce new vulnerabilities. Open-source AI models and large language models can be inadvertently or deliberately used for malicious purposes, including the design and development of harmful biological agents. The accessibility and versatility of AI tools enable both state and non-state actors to engage in activities that pose significant risks to global biosecurity (Mandile, 2022; Potter, Mossburg & Palmer, 2023).

The convergence of AI, bio-cybersecurity, and biotechnology presents the potential for global biological catastrophic risks. These risks encompass scenarios in which AI-powered activities lead to the creation of novel pathogens, viruses, bioweapons, or chemical weapons. Such developments could result in sudden, extraordinary loss of life, pose threats to national governments and international relationships, disrupt economies, challenge societal stability, and undermine global security (Mandile, 2022; Potter, Mossburg & Palmer, 2023).

It has been estimated that the scale of digital technologies has grown exponentially over the past decade. In particular, the growth of artificial intelligence (AI) and Internet of Things (IoT) devices has created a range of opportunities to 'hack' or exploit biological systems for malicious purposes (Millett et al., 2019; Palmer et al., 2021; Mantle et al., 2019). For example, AI and IoT have been used to manipulate the genetic code in plants to make them more tolerant to herbicides or to create targeted biological weapons such as genetically modified (GM) bacteria.

The use of digital technologies in the biological domain has created several cyber security risks and threats. The impact of bio-cybersecurity risks and threats can be far-reaching. For example, unauthorized access to sensitive data or gaining control of a biological system can have serious implications for human and environmental safety. Exploiting vulnerable systems could lead to the release of toxic chemicals into the environment or the manipulation of animal or plant gene sequences. Similarly, gaining control of a hospital’s computer systems could put patients’ lives at risk. The impact of bio-cybersecurity threats is not limited to human and environmental safety; the economic implications can also be profound (Millett et al., 2019; Palmer et al., 2021; Mantle et al., 2019). For example, a data breach could lead to confidential information being leaked to rival companies, or the manipulation of a biological system could result in financial losses due to lost or damaged crops or animals.

The interconnectivity between physical and virtual entities gives rise to numerous emerging threats across sectors. Cybersecurity has become an integral part of any system or network to protect data and systems from unauthorized access. Recently, we have seen a dramatic increase in cybersecurity threats in the biotechnology sector, leading to numerous data breaches in critical infrastructure (Palmer et al., 2020).

The technological landscape has been transformed over the past few decades with the emergence of Industry 4.0, digital networks, and the Internet of Things. These developments have enabled industries to create, capture and deliver value from digital technologies. However, these advances are not without consequences, as they also pose an increased cybersecurity risk to critical industries and infrastructure. The threat of data breaches due to cyber threats has become an increasingly fundamental and prominent concern today. In particular, the biotechnology sector, with its sensitive and confidential data, is particularly vulnerable to cyber threats (Palmer et al., 2020).

As the biotechnology industry plays a critical role in economic and public health development, it is subject to some unique cyber threats, mainly due to its sensitivity to sensitive and confidential data as well as its reliance on artificial intelligence, autonomous systems, and automation. Several recent incidents involving data breaches at high-profile biotechnology companies, such as Genome Corporation, Genentech, and Equinox, have highlighting the increased risk of cyber threats in this sector (Palmer et al., 2020).

The security challenges facing the biotechnology sector are multi-faceted. First, the technical complexity of such systems often makes them "harder to secure". Compromised systems can cause significant material damage, not only financially but also ethically, as sensitive biotechnological data is often used by organizations for the advancement of science and public health. Furthermore, biotechnological processes are often automated, which increases the risk of software bugs and malicious actors compromising such systems (Palmer et al., 2020).

In addition, the increasingly interconnected nature of the biotech landscape makes cross-sector cyber-attacks risky. Furthermore, the lack of awareness of cyber threats within the biotechnology sector places it at increased risk, as organizations often need to prepare to respond to such incidents (Palmer et al., 2020).

As many companies and government agencies become increasingly aware of the potential threats posed by the manipulation and misuse of information technology, they are exploring the need to significantly increase the size of their cybersecurity workforce. However, this has been challenging due to the need for more available skilled cybersecurity professionals, known as the cybersecurity talent shortage (Burrell, 2019A).

Cybersecurity and artificial intelligence have undergone a period of profound change in recent years. Technological advances have made it possible for hostile actors to obtain sensitive data from computer networks and have opened the door to the creation and distribution of malicious code. The proliferation of cyberterrorism and organized crime, both of which are on the rise, makes cybercrime a threat not only to enterprises but also to the national security (Burrell, 2019A). As a result, organisations in both the public and commercial sectors now require a larger and better-trained cybersecurity and artificial intelligence workforce to protect their data, networks, and systems from the effects of cyberattacks.

However, the difficulty is compounded by the fact that the number of qualified applicants for cyber-jobs in the United States is dwarfed by the number of

jobs, resulting in a cyber-talent shortage (Burrell, 2019A). There will be a global gap in unfilled cybersecurity and artificial intelligence jobs, and this projected deficit highlights the need for cyber professionals and an emphasis on training individuals with the necessary skills and expertise in the field. As both the biotechnology and bio-cybersecurity industries have a significant and growing need for skilled employees, this has become a significant issue in both fields.

Biotechnology and bio-cybersecurity companies faced a number of difficulties due to a skills scarcity in the field of cybersecurity and artificial intelligence. Firstly, access to skilled staff is necessary to build secure systems, implement the most up-to-date security measures and ensure that systems are constantly patched with the latest versions of available security updates. As a result, businesses may find themselves at a disadvantage to their competitors if they cannot find staff with the necessary skills to protect their systems from cyber risks (Burrell, 2019A).

As a result of this shortage, companies are increasingly competing for the available cyber and AI talent. Because of this, companies are now offering salaries to professionals with cyber expertise that are often much higher than required, which has led to additional issues with talent retention and cost inflation (Burrell, 2019A). In addition, businesses may have to make concessions, such as offering overly generous salary and benefits packages, in order to successfully recruit the most qualified candidates. This can make it difficult for companies to keep their budgets healthy in the long term.

Finally, there is a need for more competent employees in the industry, which has created an environment where it is difficult for enterprises to hire appropriate cyber capabilities, train that workforce, and keep personnel (Burrell, 2019A). This is particularly true in the biotechnology industry, which is still relatively new and highly specialized. Furthermore, many professionals with the most advanced understanding of cybersecurity and artificial intelligence are only occasionally available on the open market.

According to Mountrouidou et al. (2019) the demand for cybersecurity expertise has recently increased dramatically around the world. Currently, the job growth rate in the United States is at 28 %, which is three times higher than the national average. At the same time, the field of cybersecurity is expanding, not only in terms of technical concepts but also in terms of policy, international law, business strategy, and the human aspects of engineering. On the other hand, not much progress has yet been made in increasing the cultural diversity of the industry. The research conducted in 2019 by Mountrouidou et al. found that 24.9 % of workers hired in 2018 were women, 12.3 % were African Americans, and 6.8 % were Latino Americans.

In his work, Burrell (2020) states that organisations that want to remain relevant to their customers and competitive in the talent market must prioritize diversity in information technology (Tech) and cybersecurity. Burrell emphasizes that an inclusive work environment provides opportunities for a wider range of employees to advance their careers and reach their full potential. This is necessary to build more resilient communities and create a more equal world.

According to Horváth et al.'s research (2019), businesses are aware of the importance of diversity. However, even though businesses have collectively spent billions of dollars on diversity and inclusion projects, real change has been slow and not sustainable. The fundamental goal of diversity initiatives in information technology and cybersecurity is to “bring new points of view to an industry that is typically monolithic and frequently exclusive” (Burrell, 2019B). There is an urgent requirement for increased

representation of women and people of color in modern society. When a company has employees from diverse backgrounds, it has a greater chance of understanding its consumers (Ferreras-Perez et al., 2023; Burrell, 2021; Burrell, 2020). Customers in today's market have higher expectations of companies to provide goods and services tailored to their specific and individual needs and preferences. Conversely, employees have higher expectations of workplaces that consider their needs and value the various opinions, talents, and experiences they bring to the table (Ferreras-Perez et al., 2023; Burrell, 2021; Burrell, 2020; Burrell et al., 2023).

There is no getting around the fact that men are overrepresented in information technology and cybersecurity. Research on diversity in technology reveals that women continue to be underpaid and underrepresented year after year despite the availability of data on these topics. The situation is much more precarious for women of color. In addition, women are persistently underrepresented in leadership roles, which gradually lowers the level of satisfaction and contentment that women experience in their professions. According to Burrell (2019B), the “broken rung” effect makes it extremely difficult for women to succeed. Another critical issue is the lack of racial diversity in technology and cybersecurity (Burrell et al., 2023; Burrell, 2020; Burrell, 2021; Mountrouidou et al., 2019).

2. Problem statement

As stated by Mountrouidou et al. (2019), cybersecurity is an essential aspect of the modern economy, and its importance has increased dramatically in recent years. Following global projections, Burrell (2020) considers that there are more than one million open positions in cybersecurity. Historically Black Colleges and Universities (HBCUs) and Women's Colleges (HWCs) have been instrumental in advancing diversity and equity in higher education, having the potential to play a significant role in addressing the cybersecurity talent shortage in the United States.

As the world becomes increasingly connected through technology, cybersecurity has emerged as one of the most pressing concerns. According to Mountrouidou et al. (2019), cybersecurity specialists are essential in protecting our digital infrastructure, protecting sensitive data, and ensuring the safety and security of individuals and companies. Nevertheless, despite the increasing demand for cybersecurity specialists, the industry is still predominately occupied by men and there is a call for increased diversity (Burrell, 2019). For several different reasons, diversity in cybersecurity is significant. According to Burrell et al. (2023), for starters, diverse teams bring new perspectives and experiences, which can help to identify and manage threats that may not have been noticed otherwise. This can be beneficial to both the team and the organization. Secondly, diversity encourages creative thinking and new ideas, which is necessary in an industry that is constantly changing. Finally, diverse teams are more representative of the people they serve, which can lead to solutions that are both more successful and more equitable.

The need for cybersecurity specialists in the United States is snowballing due to the expansion of the cybersecurity industry. Higher education has become more inclusive and diverse thanks to the efforts of Historically Black Colleges and Universities (HBCUs) and Historically Women's Colleges (HWCs). These educational institutions are in a strong position to educate the next generation of cybersecurity professionals. This study examines how Women's Colleges and Universities and Historically Black Colleges and Universities, if used to their full potential, could help address talent needs and labor shortages.

3. Method

A qualitative focus group methodology was employed; all

participants were college grads working in cybersecurity. Eight had graduated from HBCUs (four women and four men), and the other eight had graduated from HWCs (all women).

The main question that guided the conversation in the small group was the following: How can HBCUs and HWCs play a role in alleviating the scarcity of cybersecurity workers?

The qualitative focus group research design is an effective tool for obtaining qualitative data from potential study participants with comparable characteristics and interests. Focus group qualitative research is an important and proven method as it enables researchers to communicate their findings quickly and effectively to a larger audience (Kitzinger, 2005; Breen, 2006; Onwuegbuzie et al., 2009). It is also particularly effective when participants are expected to meticulously examine a scenario or problem. In these circumstances, participants will be subject matter experts on a topic because of their academic training as well as their work experience.

Focus groups are designed to allow for a more in-depth examination and debate of a particular issue. The qualitative focus group research design uses this purpose of focus groups. This method is therefore advantageous as it enables the researchers to explore the participants' responses in more depth and detail (Kitzinger, 2005; Breen, 2006; Onwuegbuzie et al., 2009). In addition, this method encourages participants to have a more engaged discourse with each other, which further enhances the quality of the data.

Focused groups of subject matter experts have been used effectively by Fortune 500 companies for years. This resource provides valuable insight into current trends and the complex dynamics of emerging trends, challenges, recommendations, and potential remedies.

4. The obstacles to overcoming the strive for diversity in cybersecurity

Despite the importance of diversity in cybersecurity, the industry is still dominated by white men and lacks racial and ethnic diversity. According to Mountrouidou et al. (2019), women make up barely a quarter of the workforce in the field of cybersecurity, and the representation of minority groups is similarly low. As stated by Burrell (2020), there are a number of intricate and interrelated factors that contribute to this lack of diversity. The pipeline issue is one of the most significant challenges. Women and members of marginalized groups are underrepresented in science, technology, engineering, and mathematics professions, which are sometimes believed to be prerequisites for a job in cybersecurity. In addition, there needs to be greater understanding among young people, particularly women and members of underrepresented groups, regarding the possibility of pursuing a career in cybersecurity.

Another obstacle is the industry's continued gender and racial biases (Burrell et al., 2023; Burrell, 2020; Burrell, 2019; Burrell, 2021). According to Burrell (2019), discrimination, harassment, and microaggressions are commonplace in the workplace, contributing to the lack of representation of women and minorities as well as lower rates of employee retention. Furthermore, many women and members of minority groups working in cybersecurity believe they have to work twice as hard to establish their expertise, and they are often passed over for promotions and leadership positions.

4.1. Colleges that have a long history of providing education to women

Historically Women's Colleges (HWCs) enroll only 0.7% of all female undergraduate students in the US; nonetheless, their graduates are disproportionately represented in positions of relevance and distinction (Kiss, 2015).

According to Black Enterprise Magazine (Kiss, 2015), women who graduated from women's colleges make up 9 percent of female CEOs in the S&P 500, 10 percent of women serving in the United States Senate, and 10 percent of the Most Powerful African American Women in Corporate America. Women who graduated from women's schools also make up 9 percent of the Most Powerful African American Women in Corporate America. In addition, more than ten percent of the top seventy-five colleges and universities in the United States are women's institutions. These are the institutions whose undergraduate students acquire doctoral degrees.

Throughout their educational history, girls and women have had to fight a never-ending uphill battle to gain acceptance into traditionally male-dominated academic professions. This long-term exclusion becomes particularly evident at the advanced level. According to Kiss (2015), women have historically found it more difficult to achieve the highest levels of equality, voice, and psychological safety in higher education settings. However, they have always made up a large proportion of the student population in colleges and universities. This claim of indifference towards women in colleges and universities may be surprising, as women make up at least 60 percent of the student body on most campuses.

According to Kiss (2015), many believe that women's universities are antiquated institutions that have outlived their utility in the U.S. Although the world as we know it has undergone tremendous transformations, there are still startling parallels in the gender inequality that reigned in the past. It is therefore more important than ever to provide a female-centred educational environment (Abdulahi, 2022).

Women's colleges provide their students with a community for and about women, enabling them to impact local and communal change locally and globally (Kiss, 2015). Women's colleges also assist students in becoming more self-sufficient. There are many reasons why it is beneficial for women to attend college. Additionally, students at women's colleges report higher rates of interaction with their professors than their co-educational counterparts, who report lower rates of interaction (Abdulahi, 2022). This is in contrast to their peers attending co-educational colleges. Women's schools often cultivate an environment where students can learn from each other, even though they come from different backgrounds and perspectives on the world. According to Abdulahi (2022), universities and colleges that allow both men and women to enroll students have a greater propensity to enroll students from a wider range of racial and cultural origins. In addition, they welcome students from a wide range of socioeconomic backgrounds, which helps them maintain a high position in terms of the potential for social mobility (Kiss, 2015). At women's universities, various programs are expressly geared to assist students in developing their leadership qualities.

Female students who attend institutions and colleges designed exclusively for the education of women are more than 1.5 times more likely to major in fields related to science, technology, engineering, and mathematics (STEM) (Kiss, 2015). Faculty members who teach at women's colleges are more likely to involve undergraduate students in STEM research than faculty members who teach at any other type of schools. This is in contrast to the situation where faculty members teach at other types of schools. These schools serve children from households with lesser finances and pupils who belong to minority groups more effectively than many co-ed schools (Abdulahi, 2022).

The first women's colleges were established in the middle of the 19th century to give women access to higher education. At the time, many people believed that education was unnecessary for women whose role was in the home and that complex studies might be bad for women

(Harwarth et al., 1997). In addition, many people consider that education could be unhealthy for women.

The most prominent and prestigious women's colleges were the so-called "women's Ivy League" or the "Seven Sisters" schools: Vassar, Wellesley, Smith, Bryn Mawr, Barnard, Radcliffe, and Mt. Holyoke. These East Coast colleges were founded between 1865 and 1893 by individual philanthropists or private organizations of influential women (Harwarth et al., 1997). There are 30 women's colleges in the United States (Yang, 2022). Some notable alumnae of Women's colleges include former U.S. Speaker of the House – Nancy Pelosi, former U.S. Secretary of State – Hilary Clinton, U.S. television reporter – Barbara Walters, actress – Katherine Hepburn, author – Zora Neale Hurston, U.S. news analyst – Cokie Roberts, U.S. news reporter – Diane Sawyer, and U.S. actress - Meryl Streep.

4.2. Historically Black Colleges and Universities (HBCUs)

Even though Historically Black Colleges and Universities (HBCUs) make up only about 3 % of colleges in the United States, they enroll 12 % of all Black college students and graduate 23% of all Black college students (Goode, 2016). According to Goode (2016), a relatively small number of colleges are responsible for awarding sixty percent of all engineering degrees and forty percent of all degrees in STEM fields. They are also responsible for educating forty percent of all black health professionals and fifty percent of all black teachers in the country (Goode, 2016). Historically Black Colleges and Universities, often known as HBCUs, have proven tremendously effective in encouraging academic performance. This is especially true in the fields of science, technology, engineering, and mathematics (STEM), where students of African descent are chronically under-represented in most primarily white institutions. According to Goode (2016), HBCUs are responsible for the graduation of one-third of all African Americans who have earned doctoral degrees in the sciences. These graduates include both men and women in their entirety. They are able to do this with a much smaller amount of financial support than is provided to traditionally white organisations. This enables them to achieve their goals.

Some of the more notable alumni of HBCUs include entertainer American Idol judge Lionel Richie, filmmaker – Spike Lee, Martin Luther King Jr., 49th U.S. Vice President – Kamala Harris, NFL Hall of Fame football player – Jerry Rice, and media mogul – Oprah Winfrey, actor – Samuel L. Jackson, and Superbowl winner/Talk show host – Michael Strahan.

In his work, Bracey (2017) states that HBCUs provide cultural benefits and affordable education. The African American community has placed substantial emphasis on this cultural foundation since the turn of the 20th century. HBCUs had already established themselves as pillars of community support and educational institutions for our people (Bracey, 2017; Harris & Gaston, 2015). This was years before other universities even contemplated enrolling students of color. They cultivate an environment that values the health and happiness of their students and make it a point to actively work to build their students' self-confidence. It is possible to quantify the importance and power of a Black College or University (HBCU) education, characterised by high faculty standards, robust peer support, and a plethora of role models, and it deserves investment to maintain and enhance its quality (Bracey, 2017; Harris & Gaston, 2015).

Although many academics are aware of the achievements that HBCUs have made in the past, only a few people fully comprehend the significance of HBCUs today and in the years to come. Allen, Devost, & Mack's findings are as follows: to make HBCUs "comparable and competitive" with Predominantly White

Institutions (PWIs), the nation will need to make significant investments in HBCUs by the year 2020. Because HBCUs vary in terms of their history, financial stability, size, mission, demographics, and categorization, the assumption that there is a "one size fits all" solution must be challenged. According to Allen, Devost, & Mack (2020), some of the most significant challenges facing HBCUs today include: changing student demographics, accreditation, legislative mandates, rising costs, diminishing revenues, and updating curriculum and pedagogy. The initiative to redesign HBCUs raises concerns about how these institutions can increase student diversity while still serving the Black community and competing in the larger higher education market. There is a critical need for resources to sustain these schools and universities, particularly state HBCUs that have struggled for decades due to race-based funding inequities and that have been the subject of lawsuits and legal settlements in states such as Maryland and Mississippi (Bracey, 2017).

As stated by Allen et al. (2020), HBCUs need support to achieve financial viability and resources, and must implement entrepreneurial techniques to succeed. These initiatives include reducing reliance on unreliable or non-existent state funding, expanding external funding sources and community collaborations, strengthening institutional branding, increasing the cost-effectiveness of services, and recruiting students from a broader range of backgrounds. Many HBCUs have not yet reached a point of financial stability. This is primarily due to long-term economic deficits, an unwavering reliance on student tuition, and a lack of alternative revenue sources, such as small endowments, grants, and charitable donations. Partnerships between HBCUs and the technology industry could be a solution that could be one solution that could be a winning formula for both parties. These partnerships involve technology companies investing in HBCUs and providing infrastructure through internships, curriculum development, and technology. This would allow HBCUs to use their legacies of helping African-Americans succeed in college to develop new cybersecurity workers.

5. Recommendations collected from the focus groups

A qualitative focus group design was used with 16 college graduates working in technology. Eight were HBCUs graduates (4 women and 4 men), and 8 were HWCs (8 women). Two separate groups of 8 participants each were from HBCUs (4 women and 4 men), and 8 were from HWCs (8 women). The key questions that guided the focus group discussion were: How can HBCUs and HWCs play a role in addressing the bio-cybersecurity and biotechnology artificial intelligence workforce shortage? How can HBCUs and HWCs play a role in addressing the bio-cybersecurity and biotechnology artificial intelligence fields and workplace diversity?

6. Results

The findings are listed as key themes based on the following steps:

- Facilitated the focus group sessions, ensuring that the discussion remained focused on the research objectives. A skilled moderator encouraged participation, managed group dynamics, and probed for deeper insights.
- Sessions were video recorded for accurate data capture. Discussions were transcribed verbatim from the recordings, to preserve the richness of participants' responses.
- The initial analysis was conducted by reviewing the transcripts and notes immediately after each session. The identification of preliminary themes or patterns that emerged during the discussions was the first level of analysis.
- After each focus group session, a research team was convened for a debriefing session. This process included observations of the discussion, insights, and emerging themes.

Team discussions helped to ensure a more comprehensive understanding of the data.

- The second level of analysis included systematically coding the transcribed data by categorizing responses into themes or patterns. Three members coded independently and then compared the results.
- The process included a comparison and consolidation of codes across focus groups. The focus was on exploring commonalities and variations in participants' responses. This comparative analysis helped to refine themes and identify overarching patterns.
- The process included member checking, where participants were provided with a summary of the emerging themes to validate or refine the researchers' interpretations. This step enhanced the credibility and trustworthiness of the findings.
- The process included peer review and feedback from colleagues familiar with qualitative research methods who acted as observers. These external perspectives strengthened the rigor and validity of the study.

6.1. Theme 1: Learning through personal experience

Incorporating hands-on, real-world training into the academic programs of HBCUs and HWCs is a practice that goes back decades. This strategy emphasizes experiential education and the direct application of acquired knowledge, both of which are particularly important in the field of cybersecurity. Professionals working in bio-cybersecurity need to be fully aware of the latest technologies and methodologies and be able to apply this knowledge to real-world situations. Students attending HBCUs and HWCs can participate in experiential learning opportunities such as internships, co-ops, and research projects. These activities help students develop the skills necessary for successful jobs in cybersecurity, biotechnology, and artificial intelligence.

6.2. *Theme 2: Participation in the community*

Historically Black Colleges and Universities (HBCUs) and Historically Women's Colleges (HWCs) are in a prime position to connect with their surrounding communities and provide education and training to underprivileged people in the areas of bio-cybersecurity. Bio-cybersecurity threats do not pick and choose who they target, so everyone must have access to the information and tools they need to protect themselves and their businesses safe. Historically black colleges and universities and women's colleges and universities can serve as hubs for education and outreach, partnering with local businesses, non-profit organizations, and government agencies to promote cybersecurity, biotechnology, and artificial intelligence awareness and best practices.

6.3. *Theme 3: Education that is sensitive to different cultures*

In conclusion, HBCUs and HWCs have a long-standing commitment to providing culturally responsive education that takes into account the unique experiences and perspectives of their students. This strategy is particularly useful in the field of cybersecurity, which recognizes the importance of incorporating a variety of perspectives when formulating solutions to challenging situations. Students from minority backgrounds can make substantial contributions to the field of cybersecurity if they are prepared for successful careers in the field by HBCUs and HWCs, which emphasizes culturally responsive education. To educate, develop, and hire women and minorities in bio-cybersecurity, biotechnology, and artificial intelligence technology, corporations can form partnerships with Historically Black Colleges and Universities and Women's Colleges.

6.4. *Theme 4: Research conducted in collaboration*

In the area of cybersecurity, collaborative research initiatives between technology businesses, Historically Black Colleges and Universities (HBCUs), and Historically Women Colleges and Universities (HWCs) can provide valuable opportunities for students to engage in hands-on learning and gain real-world experience. These initiatives can help students develop the skills they need to succeed in the workplace and provide technology companies with a varied pool of talent from which to recruit new employees. By drawing on the knowledge of HBCUs and HWCs, collaborative research projects can also help technology companies stay at the forefront of research and development in bio-cybersecurity, biotechnology, and artificial intelligence.

6.5. *Theme 5: Programs for co-op employment and internships*

Another productive option for technology businesses to engage with Historically Black Colleges and Universities (HBCUs) and Historically Women's Colleges (HWCs), to train and develop bio-cybersecurity and AI expertise, is through internship and co-op programs. These programs allow students to obtain practical experience by working on projects and provide technology companies with a pipeline of intelligent, highly qualified, and diverse candidates for full-time employment. Students can gain this experience by participating in these programs. Internships and cooperative education programs give students the opportunity to network with professionals in the bio-cybersecurity field, a skill that can help secure employment in the future.

6.6. *Theme 6: Grants, fellowships, and other financial assistance*

Providing financial assistance through scholarships and fellowships is an effective way to promote diversity and equity in cybersecurity and artificial intelligence. Scholarships and fellowships can be provided by technology businesses, in partnership with HBCUs and HWCs to students pursuing degrees in cybersecurity. These programs have the potential to remove the financial barriers that prevent many students from pursuing higher education and to encourage individuals from a wide range of backgrounds to pursue careers in cybersecurity.

6.7. *Theme 7: Programs for mentors and mentees*

Mentorship programs can be a practical approach for technology businesses to work with HBCUs and HWCs to cultivate bio-cybersecurity expertise. These programs connect students with specialists in the field of bio-cybersecurity and artificial intelligence who can provide guidance and support as they work towards their educational and professional goals. Moreover, students can benefit from building valuable networks of specialists in their industry, which can be helpful when searching for future employment opportunities.

6.8. *Theme 8: Curriculum development*

Technology businesses can develop and improve bio-cybersecurity courses by partnering with HBCUs and HWCs. By providing resources and experience, businesses can assist students in their education regarding cybersecurity technologies and techniques. This collaboration also ensures that the curriculum is relevant to the needs of the industry and that students are prepared for the demands of the job market by ensuring that they are adequately equipped for the workforce. In addition, technology companies can facilitate seminars or bring in guest speakers to enhance students' knowledge of cybersecurity and artificial intelligence.

7. Conclusions

The intersection of AI, bio-cybersecurity, and biotechnology presents unparalleled challenges and opportunities for global security. As AI continues to advance, proactive efforts are needed to protect against the misuse of AI technologies for harmful biological purposes. By addressing these challenges through collaborative research, international cooperation, and ethical AI development, we can harness the potential of AI while minimizing the risks it poses to global biosecurity and stability (Mandile, 2022; Potter, Mossburg & Palmer, 2023).

Biotechnology-based systems are becoming interconnected, allowing an increasing degree of data analysis and manipulation, and malicious actors may exploit this (Millett et al., 2019; Palmer et al., 2021). Furthermore, biotechnological systems naturally have more complicated data formats, making them more difficult to be secured. On the other hand, their higher capabilities may render existing security techniques obsolete. These factors can make securing biotechnological systems challenging. Given the prevalence and importance of biotechnologies to human health, the potential for disruption of biotechnological systems has significantly greater implications than the potential for disruption of other systems (Millett et al., 2019; Palmer et al., 2021; Mantle et al., 2019).

Developing experts in the biotechnology sectors with a solid understanding of bio-cybersecurity and cybersecurity is vital for the safety and security of current systems and future systems. This is true for all the reasons mentioned above and for additional reasons. The increasing use of technology in the field of biotechnology, as well as the potential for biotechnological systems to be exploited for nefarious purposes, has resulted in an increased need for stringent security measures (Millett et al., 2019; Palmer et al., 2021; Mantle et al., 2019).

For this reason, greater emphasis needs to be placed on developing bio-cybersecurity and cybersecurity professionals with the knowledge and expertise necessary to combat emerging cybersecurity risks in this sector.

Historically Women's Colleges (HWCs) and Historically Black Colleges and Universities (HBCUs) are two educational institutions that have the potential to significantly impact the global shortage of cybersecurity professionals. In the coming years, vocations related to cybersecurity are expected to grow faster than the demand for competent workers, which is currently on the rise. These schools can provide specialized programs and information to help bridge the growing gap.

Historically Women's Colleges and Historically Black Colleges and Universities are well-positioned to contribute constructively to addressing these issues because they provide opportunities for women and members of underrepresented groups to pursue higher education in a variety of specialised fields. For instance, a women's college that is segregated by gender and has a single-gender setting can provide a safe space for students to tackle coursework that may be scary and difficult. Students at HBCUs have access to superior academic resources, and there is a more significant representation of people of color on the faculty, which helps to motivate and shape future leaders.

Both Historically Black Colleges and Universities (HBCUs) and Historically Women's Colleges (HWCs) play an essential role in ensuring access to higher education by lowering tuition costs and supporting African American students interested in pursuing degrees and careers in science, technology, engineering, and mathematics (STEM) fields. HBCUs and HWCs are referred to as "Historically Black" and "Historically Women's" Colleges and Universities, respectively. By attending HBCUs or HWCs, where tuition is typically more affordable due to lower

tuition costs or generous financial assistance packages, students are better able to keep their overall debt under control. Even the historically black colleges and universities, which have some of the highest tuition rates in the country, charge less than the typical rate for all schools. Even if they are from out of state, students attending several public HBCUs, including Alcorn State University, Grambling University, and Jackson State University, are eligible for in-state tuition rates and associated fee reductions.

Evidence shows that students' mental health improves at Historically Black Colleges and Universities (HBCUs) and Historically Women's Colleges (HWCs). This is most likely because students at these institutions are exposed to less overt racism and microaggressions. HWCs and HBCUs invest in creating a shared experience and culture for their students, which results in an improved academic atmosphere. HWCs and HBCUs have alumni networks with more people who appear like their current students. Therefore, these universities have the potential to play a significant role in educating and developing a larger pool of future talent to overcome the skills gaps that currently exist in the cybersecurity industry.

Diversity in the cybersecurity and artificial intelligence workforce is essential to prevent a deficit in knowledge transfer and insight, and institutions of higher education should lead the way in developing a more inclusive and diverse cybersecurity atmosphere. The cybersecurity and AI workforce needs to reflect a wide range of experiences and viewpoints to keep pace with the industry's ongoing evolution, which requires the dissemination of knowledge and development of new technologies. Women's Colleges and Universities, as well as Historically Black Colleges and Universities, will continue to be vital resources for skilled researchers and perceptive practitioners.

REFERENCES

Abdulahi, S. (2022). Unicorns' in Uncertain Times. *Inside Higher Education,* available at: https://www.insidehighered.com/news/2022/11/30/womens-colleges-work-maintain-their-mission.

Allen, W.R., Devost, A., & Mack, C. (2020). Hidden in plain sight: Historically black colleges and Universities in America. *Quaderni di Sociologia*, *Vol. 64, No. 83-LXIV*, 25-46.

Bracey, E.N. (2017). The Significance of Historically Black Colleges and Universities (HBCUs) in the 21st Century: Will Such Institutions of Higher Learning Survive? *Am J Econ Sociol, Vol. 76, Issue 3,* 670-696. Available at: https://doi.org/10.1111/ajes.12191.

Breen, R.L. (2006). A practical guide to focus-group research. *Journal of Geography in Higher education*, *Vol. 30, Issue 3*, 463-475.

Burrell, D.N. (2019A). How Hiring Baby Boomers Can Assist with the Global Cybersecurity Employee Shortage. *International Journal of Hyperconnectivity and the Internet of Things*, *Vol. 3, Issue 2*. Available at: https://go.gale.com/ps/i.do?id=GALE%7CA760411720&sid=sitemap&v=2.1&it=r&p=AONE&sw=w&userGroupName=anon%7E212c9297&aty=open-web-entry.

Burrell, D.N. (2019B). Developing more Women in Managerial Roles in Information Technology and Cybersecurity. *MWAIS 2019 Proceedings*, *20*. Available at: https://aisel.aisnet.org/mwais2019/20/.

Burrell, D.N. (2020). An exploration of the Cybersecurity Workforce Shortage. In *Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications,* 1072-1081. IGI Global.

Burrell, D.N. (2021). Creating Diverse and Religiously Inclusive Workplace Cultures in Hyper-Connected, Technical, and Cyber-Driven Organizations. *International Journal of Sociotechnology and Knowledge Development (IJSKD), Vol. 13, Issue 3*, 17-32.

Burrell, D.N., Aridi, A.S., & Nobles, C. (2023). Diversity Leadership Development for Cybersecurity Managers in Healthcare Organizations. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems,* 240-254. IGI Global.

Ferreras-Perez, J., Burrell, D.N., Nobles, C., Aridi, A.S., Richardson, K., & Khanta, K. (2023). Retaining Generation Z Cybersecurity Talent in Government and Beyond. In *Handbook of Research on Cybersecurity Risk in Contemporary Business Systems,* 325-342. IGI Global.

Goode, R. (2016). The HBCU Debate: Are Black Colleges & Universities Still Needed?. *Black Enterprise*, 1-2. Available at: http://www.blackenterprise.com/lifestyle/are-hbcus-still-relevant.

Harris, G.J., & Herron Gaston. (2015). The Enduring Relevance of HBCUs in America. *Huffpost College*, 23: 1-5. Available at: https://www.huffpost.com/entry/the-enduring-relevance-of_b_6498282.

Harwarth, I., DeBra, E., & Maline, M. (1997). *Women's colleges in the united states: History, Issues, & Challenges*. Diane Publishing.

Horváth, Z.E., Szakács, A., & Szakács, Z. (2019). Insider Research on Diversity and Inclusion: Methodological Considerations. *Mednarodno inovativno poslovanje = Journal of Innovative Business and Management, Vol. 10, No. 1*. DOI:10.32015/JIMB/2018-10-1-3.

Kitzinger, J. (2005). Focus group research: using group dynamics to explore perceptions, experiences and understandings. *Qualitative research in health care, 56-70.*

Kiss, E. (2015, June 24). Women have already achieved educational equality. But women's colleges still matter. *The Washington Post*. Available at: https://www.washingtonpost.com/posteverything/wp/2015/06/24/women-have-already-achieved-educational-equality-but-womens-colleges-still-matter/.

Lynch, M. (2015, March 6). Why the U.S. College Landscape Still Needs HBCUs. *The Huffington Post*. Available at: https://www.huffpost.com/entry/why-the-us-college-landsc_b_6478384.

Mandile, A. (2022). *A blurring line between biological and cyber threats: a legal analysis of the international cyber-biodefence strategy*. Luiss Thesis.

Mantle, J.L., Rammohan, J., Romantseva, E.F., Welch, J.T., Kauffman, L.R., McCarthy, J., Schiel, J.E., Baker, J.C., Strychalski, E.A., Rogers, K., & Lee, K.H. (2019). Cyberbiosecurity for Biopharmaceutical Products. *Frontiers in Bioengineering and Biotechnology, Vol. 7*. Available at: https://www.frontiersin.org/articles/10.3389/fbioe.2019.00116/full.

Millett, K., dos Santos, E.F., & Millett, P. (2019). Cyber-Biosecurity Risk Perceptions in the Biotech Sector. *Frontiers in Bioengineering and Biotechnology, Vol. 7*. Available at: https://www.frontiersin.org/articles/10.3389/fbioe.2019.00136/full.

Mountrouidou, X., Vosen, D., Kari, C., Azhar, M.Q., Bhatia, S., Gagne, G., Maguire, J., Tudor, L, & Yuen, T.T. (2019). 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*, 157-176. DOI: 10.1145/3344429.3372507.

Onwuegbuzie, A.J., Dickinson, W.B., Leech, N.L., & Zoran, A.G. (2009). A qualitative framework for collecting and analyzing data in focus group research. *International journal of qualitative methods*, *Vol. 8, Issue 3,* 1-21.

Palmer, X., Potter, L., & Karahan, S. (2020). On the Emerging Area of Biocybersecurity and Relevant Considerations. *ArXiv, abs/2003.12132*.

Palmer, X., Potter, L., & Karahan, S. (2021). COVID-19 and Bio-cybersecurity's Increasing Role on Defending Forward. *Int. J. Cyber Warf. Terror., 11*, 15-29.

Potter, L., Mossburg, K., & Palmer, X.L. (2023, June). A Reflection on Typology and Verification Flaws in Consideration of Biocybersecurity/Cyberbiosecurity: Just Another Gap in the Wall. In *ECCWS 2023 22nd European Conference on Cyber Warfare and Security*. Academic Conferences and publishing limited.

Yang, H. (2022, April 29). The Power of Historically Women's Colleges. *The Women's Network*. Columbia University. Available at: https://www.thewomens.network/blog/the-power-of-historically-womens-colleges.