Diversity Versus Its Influence on Cybersecurity

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Eli Bryant Roberts

Spring 2025

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Karina Rider, Department of Engineering and Society

Introduction

As a minority in America, I have found it difficult finding people in the cybersecurity workforce that look like me. Pursuing a computer science undergraduate degree and a cybersecurity focal path, I question why there is a lack of diversity everywhere I go. In a world filled with diversity, I feel as if I am being my own self advocate.

Given that diversification has statistically shown that it improves performance and outcomes at work, this issue should have already been addressed (Gomez & Bernet, 2019). The gap between zero-day attacks versus the vacant cybersecurity positions that are unfilled is tremendously concerning. In a world filled with technology, why are we not able to protect our data? Better yet, why are people having a hard time breaking into the cyber industry?

It is often said that inclusion in the workspace or lack of role models is the reasoning behind this diversification; while this is true in some sense these are only consequences for why diversity is not occurring.

The root issue is from the lack of preparation and exposure. If someone wants a career in cybersecurity they either A. do not know how to get in because of the lack of guidance or B. start their cybersecurity journey and end up giving up because they do not have efficient resources or support.

To justify my reasoning I will be pulling from various scholarly articles and investigations to prove my point. I will be using statistical data found from other researchers to show why representation is lacking in cybersecurity and how this can be fixed. I will also be including along the way my own personal experiences and how the data that I have gathered has correlated directly to what I have discovered.

Attack plans that Trump's advisors have released via Signal were plastered across the internet. Are we really prioritizing the security of our digital information seriously? My answer is no but let's get into it.

Background and Content

Everything in today's world revolves around the expansion of technology. From cloud server providers making data centers to using VLANs to segment different hosts in a small business, technology is at the forefront for these operations. This diversification of technology leaves vulnerabilities open to be exploited. Now here is where things start to not make sense.

If diversity is important and technology is the backbone of Americans infrastructure, why are we not looking for a way to fix this?

A research study found that "2,300 security managers reported that 59% of their security positions were unfilled, although 82% anticipated cyberattacks to their systems" (Mountrouidou et al., 2019). From common talk especially at UVa, it's rare to hear someone pursue a field in security or IT. Even from my own personal experience, being someone who is pursuing cybersecurity rather than aspiring to be a software engineer, I feel as if I am being looked at cockeyed. Saying that cybersecurity is important is one thing, but actually implementing actions to show this is another.

In order to understand my argument, please keep these two facts in mind. The first being that diversity is important and the second is that technology is growing at a rapid rate. Not only are these technologies ubiquitous, but they are also highly vulnerable. You want to make an online purchase from the comfort of your own home? You need a secure network to do so. Do you have a fancy bluetooth refrigerator? Even that needs a secure network. Devices are becoming more automated for faster customer consumption, and with technology becoming

more diverse so is the risk for these machines to have bugs and vulnerabilities. Diversity has been shown to improve workforce performance, it is not a myth, it is a well known fact (Gomez & Bernet, 2019). The more people working together with a variety of skills and perspectives allow for better problem solving. Faster and more efficient problem solving would allow for better protection especially with cybersecurity.

Tables 1 and Table 2 present data on the composition of the current cybersecurity and computer-based workforce in the United States. Table 1 illustrates the distribution of individuals in cybersecurity and STEM positions by race, indicating a workforce predominantly composed of white employees. Table 2 highlights the gender disparity within the IT workforce, revealing a significant gap. These data, derived from a research study, suggest that the cybersecurity and IT sectors currently lack diversity, with representation leaning towards white male employees (Chamlou, 2022)

RACE OF EMPLOYEES	% OF ALL JOBS	% OF ALL STEM JOBS	% OF COMPUTER SCIENCE JOBS (INCLUDING CYBERSECURITY)
White	63	67	62
Asian	6	13	20
Black or African American	11	9	7
Hispanic or Latino	17	8	8
Other	3	3	3

Table 1: Distribution of cybersecurity & STEM jobs based on race

GENDER OF EMPLOYEES	% IN CYBERSECURITY CAREERS
Man	76
Woman	24

Table 2: Distribution of cybersecurity jobs based on gender

Methods & Theoretical Framework

The methods I used for collecting this data was all through online research. Where I collected my data was by looking at Google Scholar articles and doing some basic high level research via Google. When I wanted to find actual statistical data, I used Google Scholar. Whereas when I wanted to collect high level information I just did a basic Google search. Majority of the time I looked up "diversity in cybersecurity" and using each webpage via snowballing for my research. Majority of my data was statistical data like graphs and other charts regarding the percentage of who is working in cyber and comparing the difference. I only used data that was deemed as relevant and from reliable sources. Some data that I did come across seemed informal but the sources were not trustworthy so I ended up not using them. Majority of the high level concepts (why is there a lack of exposure for cybersecurity in minorities, etc) I used scientific articles and my own personal experiences to back it up. As a current undergraduate who is learning how to maneuver around cybersecurity, I found this argument as a great way to also express and validate what I have been going through on my cybersecurity journey.

Throughout my research I used autoethnography in order to obtain and find my data. Autoethnography is where researchers "seek to describe and systematically analyze personal experience in order to understand cultural experience" (Ellis, 2011, p. 1). Given that a lot of the data that I have found correlates with my own life experiences, it was easier to identify noticeable patterns and issues from the get-go. While using my life as a pathway to discover any relevant information, this allowed me to connect these findings to broader trends/additional data.

The theoretical framework that aligns best with my findings is intersectionality. This framework is based upon the idea that all oppression is linked together (Taylor, 2019). Throughout my research, I found that our technological advancements where the reason behind why there is a digital skill gap in today's world. The technology in our society is consistently being altered and

improved, with that being changed so is our culture and how we adapt to it. There is a huge technological skill gap in regards to people being joining the workforce (Cybersecurity and other industries included) and because of this the data shows. Since people are not fully capable in practicing these digital skills, it is harder for people to get into cybersecurity. So difficult the norm throughout the internet is how to “break into cybersecurity”. With the digital gap increasing so is the gap for diversity in the cyber workforce.

Findings & Analysis

The lack of inclusion and exposure has a direct impact on the gender and race gap for all minorities aspiring to join the cybersecurity workforce. From the lack of resources to the non present role models, all of these factors contribute to why cybersecurity is lacking in diversity.

One of the most prominent issues is the difficulty to access education and training. As a current person of color looking for training for these entry level cyber security positions, it is hard. Yes there are resources available but I feel like I’m playing a treasure hunt to do so. When I even began my cybersecurity focal path at UVa, that was only by accident when my intro to cybersecurity professor told my peers that this was an avenue that could be taken. The cyber focal path that I am doing currently is a great way for me to learn about cyber based topics but in order to even receive that information you need to be in college to do so. For people who are not in college or can not afford going to university, it’s going to be hard to receive this education.

Outside of the realm of college, there are alot of barriers that need to be overcomed to even attempt to break inside cybersecurity. Below is a chart depicting the five types of security courses containing their respective costs (Bui, 2024). Certifications being one of the standard prerequisites range from 370-4,000 dollars. Keep in mind this is usually including just paying for

an exam voucher. So if you do not pass on the first go around, a 400 dollar exam could be 800 if not prepared appropriately.

Type of Cyber Security Course	Average Cost Range	Key Highlights
Bootcamps	$2,500 – $17,000	Intensive, short-term programs for quick entry
Online Courses	$5,000 – $20,000	Flexible, self-paced, with hands-on training
University Degrees	$3,225 per term – $47,400	Comprehensive knowledge, often with online options
Vendor-Specific Training	$300 – $3,500	Focus on specific tools or vendor platforms
Certifications	$370 – $4,000 (exam & training)	Credential-focused with varying experience levels

Table 3: Cybersecurity courses based upon cost

Aside from my own cyber electives, a lot of my training is outside of the school curriculum. The CompTIA, which is basically an organization that specializes in exams for cyber based topics, is a great way for people to tell employers that they are qualified in a specific concept in IT. These exams are ridiculously expensive; I took & passed the CompTIA Security+ exam which costs 400 dollars on average. It took me six months to fully understand and retain all of the information. Basically what I am saying is that you need to be really motivated to get these certifications or your chances of being chosen for an interview are going to be way harder. The offensive security certified professional, OSCP, is also a very well known certification for people wanting to become an ethical hacker. Like many others (and myself included), the idea of becoming a hacker is usually why people become interested in working in cyber. This certification costs almost two grand but this is the golden ticket for becoming a penetration tester. Now this is an amazing hands on certification to take but nobody is going to pay for this if they

do not have any guidance or knowledge in cyber in the first place. Keep in mind - these are just the prerequisites for just getting a job in cybersecurity. Cyber Security jobs need certifications, certifications need money, people who lack money will not be as inclined or able to pursue these certifications for a higher education. There is a ton of content on the internet that could aid people in joining the cyber workforce, but it can get overwhelming and misconceptions can be made without a proper guide.

There are a lack of role models in cybersecurity and the diversification of the current workforce directly reflects that. Research was conducted saying that “girls' interest in STEM nearly doubles when they have role models in the field, according to a European study of girls and young women ages 11-30” (Brussels, 2018). How do we expect people to work in cyber if they do not have other people doing the same? People without role models will perceive the industry and themselves differently because of it. Having a mentor or some sort of role model provides guidance and support for children to join the cyber world.

Without this positive reinforcement children are more likely to look at social media for representation which can “show prejudice and bias toward certain demographics” (Allen, 2022). Since cybersecurity is already a white male dominated field, a person of color seeing this on social media is going to have a harder time seeing themselves and saying “I can do this”

Absent positive reinforcement or actual guidance is the byproduct of misconception. Working in cybersecurity does not mean you are Mr. Robot. That's a huge misconception that is consistently being spread across the internet and it is hard to differentiate between if you do not know its true. You do not need to be amazing at coding to work in cybersecurity and social media does not shine light on that. Without knowing this, people automatically have this idea that to work in cyber you need to be a genius at coding. I, myself, am not perfect at coding and I

had the same misconception. But after pursuing this career and field I learned that there is a wide range of jobs for people regardless of your skillset and background. Aside from that, if you do not know what's true or false via the internet, it's going to be difficult to make an accurate decision on if cybersecurity is for you or not.

One hollywood hacker myth is called the lone wolf hacker. The idea is that a hacker is viewed “as a solitary genius who can solve any problem on their own.” (Ubiminds, n.d). This hacker is usually portrayed as someone who is a mastermind who is able to bypass a firewall within seconds of inspection. The most famous example via media is whenever they break into a server (randomly spitfire some words onto their computer) and then saying “I'm in”. This misconception, just like all of the others on social media, is why there is this idea that you need to be an all around tech wiz to be a part of the IT department.

I perceive this cybersecurity dilemma as a domino effect, all of these factors are caused by exposure. If education was easily accessible and was not so expensive, people who are interested in pursuing a career in IT would be more open to the idea. Since this is not the case, there is a digital skill gap where there are unfilled security positions versus continuous threats and bugs that are being discovered by hackers. Without proper pathways or guides to help people of color be able to join this industry, it makes it an obstacle to get an education to receive an entry level position. Finally the lack of minorities in cybersecurity now makes it way easier for misconceptions to be perpetuated which in the end will push people away from trying to work in IT all together.

If you still are not convinced about my claim, let's talk about some actual interviews that were actually conducted on computer science students and their perspective on cyber.

At the Florida Institute of Technology twenty-three students underwent interviews in regards to retrieving a qualitative analysis on each URM, underrepresented minority, asking about their experience with CS and cybersecurity (Osmanet al., 2023). These participants were six URM professionals already working in IT, six URM college students pursuing CS or software engineering, one high schooler, and ten college professors who were within the Computer science department. After going through these surveys the researchers provided numerous recommendations for practice before future reference. Here are a couple that stood out that should definitely be highlighted:

1. Expose URMs to CS and programming
2. Promote persistence
3. Provide social support
4. Leverage URM representation
5. Build communication skills
6. Train using real-world application

For me this list just continues to validate how much of an importance exposure and preparation is for people of color. The one that really stuck out to me from this list is building communication skills. I feel as if this communication is not really discussed or worked on but the saying “communication is key” is really essential, especially for people working in cyber who are protecting our server and data

The most important and valuable recommendation would be exposing URMs to CS and programming. From my own experience, I was only introduced to computer science at the end of my high school career. I was lucky enough to get accepted into my engineering academy in 12th grade which gave me access to experiment with MatLab and Arduino early on. But if I was not

given this opportunity my first exposure to coding would have been my first year of college. This is way too late for URMs to be exposed to technology. A Lot of public schools do not provide children the opportunity to experiment with enhancing their computer science skills. If you have never coded before, how are you going to know if you want that to be your career? This question can also be refactored and asked about cybersecurity; If children have never been taught IT security, how do you expect them to want to pursue a career in that field?

The next recommendation that stood out was providing a social support system. From my own experience, having some sort of outlet is a huge way to receive help. A lot of influencers and content creators are using their own platform as a way to promote unity to help cultivate a safe place for people of color and underrepresented people to join cyber. Although these are all great, they still need to become more mainstream and accessible. By implementing more outlets for social support, this would allow for a better community and more people would be more open to staying connected with other cyber professionals.

Another interview from the cyber professionals mentioned that they “ended up doubting myself more than my peers and had imposter syndrome. The worst was when I got hired at a big tech company, and I was told that I was a diversity hire” (Osman et al., 2023). Just like the cybersecurity professional who has already broken into the industry already, this same situation happened to me! I applied and was accepted to my engineering program during my junior year of high school and someone told me that I was just the diversity hire as well.

Another URM student discussed how their engineering professor “lost its only female professor. We were surrounded by men. There were seven girls when I started, only two graduated as the rest switched out. It gets hard when you don't have anyone to relate to.” Just like

this URM I can also vouch and say that I also have only had two CS professors teach me during my four years while attending university.

So what? What I am getting at from this investigation is that this lack of diversification is happening everywhere, and this can be seen especially in college, which can have a long lasting impact on people of color who are actually in the cybersecurity field.

Another example of where this can be found is from a working group report published in 2019. This report gave recommendations for boosting diversity in cybersecurity education for education researchers. In this report three research questions were being dissected. These questions were:

1. What is the current body of work concerning the diversification of the cybersecurity field?
2. What are the gaps in education research for diversification of the cybersecurity field?
3. What approaches are successful or unsuccessful in diversifying the cybersecurity field?

After conducting their research multiple things were recommended. Summer camps, pre college activities and introductory courses were all advised for further development. What do all of these activities all have in common? Exposure! All of these activities were individually discussed on how they would help URM children to better improve their knowledge on their cybersecurity skills. A survey was also conducted and here are the answers depicted in graph form.

In Figure 1 here you can see the observed measurements that were derived from survey data. This data was all pulled from people who are currently in the cybersecurity workforce

which was used to highlight disparities in minority representation within the cybersecurity field. This visual representation underscores the need for diversification efforts in cybersecurity education and workforce development. Each of the data values were made into a bar graph and separated by diversity characteristics.

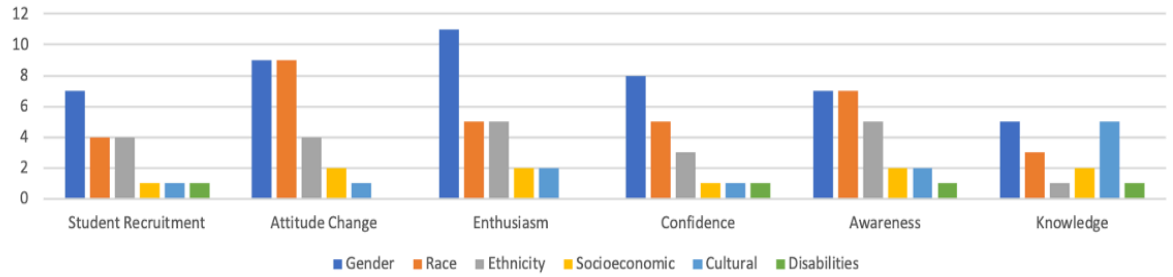

Figure 1: Observed measurements of effectiveness in surveyed papers, separated by diversity characteristics.

Conclusion

Cybersecurity is the backbone of American infrastructure, in order to strengthen this and reduce the technological skill gap, diversity needs to be increased. The way for this to be accomplished is through exposure. How can this be accomplished? I think our government and our educational institutions could do a better job than what they are doing now to implement these concepts to our children.

Our current state of our government is in shambles and it's having a huge impact on our national security. Just recently war plans were plastered across the internet and this was due to Trump’s advisors. Seriously? If we can not protect war plans from being leaked, how do we expect to transmit or store our personal data without the worry of it being stolen? Just as Trump's advisors leaking our sensitive data to the internet, this is a huge representation for how much work cybersecurity needs to be improved as a whole.

What stands out is the lack of action being taken to fix this diversity issue. There is so much information about how to increase diversity and why there is an issue but I do not see anything in regards to people wanting it to change. Trump being in office and DEI not being valued has definitely a huge impact, what I keep on asking myself is why? What's the point of saying diversity is lacking and explaining its importance but not making any steps to actually do so. Why are we not addressing the issue at hand?

It could be that people are just not educated enough to know why there is a lack of diversity in cybersecurity. Or it could just be flat out the government knows but they honestly do not care enough to give the resources to help the cause. Either way, Cybersecurity needs to be improved and having more diversity via exposure can easily solve this problem.

References

Allen, B. (2024, August 13). *Minorities and the Cybersecurity Skills Gap*. Forbes. https://www.forbes.com/councils/forbestechcouncil/2022/09/30/minorities-and-the-cybersecurity-skills-gap/

Brussels. (2018, April 25). *Role models vital in keeping European girls' stem interest alive*. Microsoft News Centre Europe. https://news.microsoft.com/europe/2018/04/25/role-models-vital-in-keeping-european-girls-stem-interest-alive/

Bui, S. B. (2024, November 21). *Cyber security course cost: 5 top course options to explore*. F. Learning Studio. https://flearningstudio.com/cyber-security-course-cost/#:~:text=Generally%2C%20the%20cost%20ranges%20from,%2C%20or%20online%20courses%2C%E2%80%A6

Coombes, H. (2020, October 15). *Intersectionality 101: What is it and why is it important?*. Womankind Worldwide. https://www.womankind.org.uk/intersectionality-101-what-is-it-and-why-is-it-important/

Ellis, C., Adams, T. E., & Bochner, A. P. (2011). Autoethnography: An Overview. *Historical Social Research / Historische Sozialforschung*, *36*(4 (138)), 273–290. http://www.jstor.org/stable/23032294

Jeffrey Goldberg, S. H. (2025, March 31). *Here are the attack plans that Trump's advisers shared on signal*. The Atlantic.

https://www.theatlantic.com/politics/archive/2025/03/signal-group-chat-attack-plans-hegseth-goldberg/682176/

Mountrouidou. (2019, December 18). *Securing the human | proceedings of the Working Group reports on innovation and Technology in computer science education*. Securing the Human: A Review of Literature on Broadening Diversity in Cybersecurity Education. https://dl.acm.org/doi/abs/10.1145/3344429.3372507

Osman, M. C. (2023, October). Understanding How to Diversify the Cybersecurity Workforce: A Qualitative Analysis . chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=1145&context=jcerp

P;, G. L. (n.d.). *Diversity improves performance and outcomes*. Journal of the National Medical Association. https://pubmed.ncbi.nlm.nih.gov/30765101/

Why diversity in Cybersecurity Matters. Explore Cybersecurity Degrees and Careers | CyberDegrees.org. (2022, November 16). https://www.cyberdegrees.org/resources/diversity-in-cybersecurity/