THE HEWLETT FOUNDATION'S CYBER TALENT PIPELINE

An evaluation based on Equitable Evaluation Framework™ principles

Jodi Nelson and Claire McGuinness

April 2021

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The William & Flora Hewlett Foundation designs both long term program strategies and fixed-period initiatives to fulfill its objectives. In 2013, Hewlett president Larry Kramer decided to transition the then sunsetting Nuclear Security Initiative to focus on cybersecurity. In 2014, program Director Eli Sugarman joined the foundation to lead the new Cyber Initiative team's efforts to develop a grantmaking strategy to build the institutions, experts and policy infrastructure the team believed necessary to enable effective cyber policy into the future. The largest part of the grant portfolio was allocated to the *Talent Pipeline* – grants intended to help universities produce experts with the skills to populate the cyber policy workforce.

As the Initiative approached its final few years and before he transitioned out of the foundation, Sugarman commissioned this evaluation to take stock of the portfolio's progress and deepen the team's understanding of the models that developed across grantee universities. Under Sugarman's leadership, the evaluation objectives were defined to center on questions of diversity and equity. More specifically, the evaluation focuses not only on whether the foundation delivered on its original intention, but also explores what it would take for Hewlett and other donors to contribute to a diverse, equitable and inclusive cyber field moving forward.

We develop a taxonomy to help describe and analyze the foundation's grantee portfolio within a larger map of cyber programs. We compare Hewlett-funded cyber programs to non-Hewlett programs according to three dimensions: interdisciplinarity; formality; and prioritization of diversity, equity and inclusion. We chose these factors to drive our landscaping because of the Cyber team's interest in multidisciplinary education, its hope to support enduring programs, and its commitment to understand how best to improve diversity, equity and inclusion. We find that despite real bureaucratic barriers that exist for university program leaders pursuing formal, interdisciplinary education, 10 of Hewlett's 23 domestic university grantees have made significant progress. However, although diversity is vital to cyber policy, fewer than 6 Hewlett-funded programs have pursued relevant actions and outcomes as an integral part of their cyber programs. As part of our analysis, we provide case studies of promising practices used by both Hewlett grantee and non-grantee program leaders in all three of these core areas.

The heart of the insights we gained applying the principles of the Equitable Evaluation Framework™ center on the weight and implications of philanthropic strategies that are based on concepts that assume away the structural inequity that many people face accessing education and employment in a field like cyber.[1] We use the insights we gained to create two strategic frameworks that offer alternative framings to the "pipeline" concept that informs the Cyber team's theory of change and assumptions. We learned that philanthropic strategies that do not take stock of the barriers to opportunity that many people face can unintentionally exclude those same people. The frameworks we present identify both the specific barriers people identified, and the interventions they shared as ideas for philanthropic investment.

The final section presents recommendations to both Hewlett and other funders interested in investing in an effective, diverse and more equitable cyber field. Appendices include case studies of university programs and practices as well as illustrative programs and organizations working to promote a diverse and equitable cyber field.

[1] "Equitable Evaluation Framework™", *Equitable Evaluation Initiative*.

I INTRODUCTION

Background

Larry Kramer began his tenure as president of the William and Flora Hewlett Foundation at the same time the US government prioritized cyberattacks above international terrorism in the catalog of dangers facing the country.[2] In October 2012, US Defense Secretary Leon E. Panetta warned that the United States was facing the possibility of a "cyber-Pearl Harbor" and was increasingly vulnerable to foreign computer hackers who could dismantle the nation's power grid, transportation system, financial networks and government.[3] Over the next few years, cyberattacks increasingly threatened corporate, government and international boundaries, motivating the US government to expand its cybersecurity force. Among the key challenges agencies faced were how to find, train and retain a large number of qualified people who could navigate this evolving area of national and corporate security.

Kramer had been aware of growing government and business concern with cyber threats when he joined Hewlett. In his own words, "problems in government and industry were growing but the people responsible for them were fully occupied just putting out the latest fire. Nobody had time to think about long-term policy, and this risked creating a path dependency where short term decisions would affect the future." Once a foundation landscaping revealed that there was no philanthropic funding to help fill this capacity gap, Kramer and his team established a new initiative to do just that: "to develop a field of institutions staffed by people with the necessary training and opportunity to think about long term national and global cyber policy."

Eli Sugarman joined as program director of the new Cyber Initiative in 2014. Sharing Kramer's insight that the Hewlett Foundation had an opportunity to "build a field of experts that can come up with the analytic frameworks to have an informed debate and therefore prevent short-term, reactionary policy decisions," Sugarman developed a grantmaking strategy to build the institutions, experts and policy infrastructure the team believed necessary to enable effective cyber policy into the future. The largest part of the grant portfolio was allocated to the *Talent Pipeline* – grants intended to produce experts with the right skills to resolve the shortage in the cyber policy workforce.[4]

The Hewlett team joined others who believe that the nature of cybersecurity requires multidisciplinary education and training because the vulnerabilities, risk, relevant legal frameworks and potential policy solutions facing companies and governments cannot be addressed by experts of one discipline – such as computer science or law. Decisions made to protect a firm or government agency from cyber threats cannot be made by only addressing technical vulnerabilities, and cybersecurity policies have impacts on people and potentially long term legal and normative implications.[5] This insight guided the Cyber team's decision to support university programs with a commitment to multidisciplinary education and training. Given the newness of the field and lack of a blueprint for what constitutes a "good" cyber program or how to develop one, the Hewlett team supported different types of programs in order to understand the combination of disciplines, faculty, initiatives and classes that would be most impactful in producing the necessary talent for the future.

By 2020, the Cyber team had spent $59 million to support 23 domestic university-based multidisciplinary cyber programs.[6] With the Initiative set to come to a planned end in 2023, Sugarman and his team commissioned this evaluation to learn how the foundation delivered on its intention. In light of the 2020 racial justice movement and the foundation's commitment to diversity, equity and inclusion (DEI), the team elevated evaluation questions related to diversity and equity, seeking to understand for whom the Hewlett

[2] Mazetti, Mark and David Sanger, "Security Leader Says US Would Retaliate against Cyberattacks." *The New York Times,* March 12, 2013.
[3] Bumiller, Elizabeth and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times,* October 11, 2012.
[4] See the Initiative's full strategy here.
[5] Jean Blair R.S., Andrew O. Hall and Edward Soblesk. "Educating Future Multidisciplinary Cybersecurity Teams." *Computer*, Volume: 52, Issue: 3, March 2019.
[6] There are 27 Talent Pipeline grantees. For the purposes of this evaluation, we focus on the 23 domestic university programs.

talent pipeline is working and why; which groups and communities are not being well-served; where the foundation team did and did not make progress in terms of integrating equity, inclusion and diversity into its approach and outcomes; and where it fell short.

Evaluation design

This evaluation was designed to fulfill these objectives and provide actionable findings for the foundation, university program leaders and prospective funders interested in supporting the ongoing development of a robust, high quality, diverse, equitable cyber policy field.

Three evaluation questions guided the data collection and analysis.

1. Where are we now? - What is the current state of Hewlett's talent pipeline, and the larger landscape of university cyber programs? What is working well and what is not, and why? What groups are well-served by the pipeline?
2. How did we get here? - What factors have driven the pipeline's development? How effective was Hewlett's approach, and what role did its assumptions play? How did that effect which stakeholders were served and why?
3. Where do we go now? - What opportunities exist to further build the pipeline in the future? What gaps still exist, particularly in who Hewlett is serving? What are the approaches and lessons learned that can be shared with other funders as Hewlett prepares to exit the field?

While traditional evaluation summarizes and analyzes progress and learning, equitable evaluation seeks to advance equity as an end in itself.[7] This requires asking questions to understand how different populations experience outcomes and to identify structural drivers of inequity. Key to an equitable evaluation is assessing not only what occurred, what worked and why, but also for whom. While still client driven, an evaluation that applies Equitable Evaluation Framework (EEF) principles intentionally surfaces that solutions impact people in different ways and are not universally beneficial.[8] Even if a client decides not to act on alternative solutions identified through the inquiry, the evaluator's role is to encourage them to consider the rationale and articulate why they are not.[9]

These principles informed the sampling and methodology of the evaluation. We identified a sample to capture perspectives that the foundation might not have previously heard. The sample included grantee and non-grantee cyber program leaders; employers who recruit cyber talent; cyber professionals of color; and leaders who work at organizations with a mission to improve diversity and equity in the cyber sector or higher education more generally. We interviewed 66 individuals. The number and breakdown of these categories are presented in Table 1; names and affiliations are presented in the appendices.

Table 1: Sample of Key Informants

Category	Interviews
Hewlett staff	4
Grantee university programs	24
Non-grantee university programs	15
Cyber employers	5
People of color in cyber policy	12
Diversity, equity and inclusion experts	6
TOTAL	**66**

[7] J. Dean-Coffey, J. Casey, & L. D. Caldwell, "Raising the Bar — Integrating Cultural Competence and Equity: Equitable Evaluation", *The Foundation Review*, 6(2), 81–94, 2014.
[8] "Equitable Evaluation Framework™", *Equitable Evaluation Initiative.*
[9] Julia Coffman, "Equitable Evaluation is for All", *Equitable Evaluation Initiative,* October 2019.

We used a variety of methods to identify this sample. We did our own research and used snowball sampling to identify non-grantee university programs. To identify employers, we combined the Cyber team's recommendations with our own research. And to identify DEI experts and people of color working in cyber, we researched affinity groups, identified members and participants at DEI-focused events in the field.

We used key informant interviews, Hewlett's grantee surveys and published literature on related trends as key sources of data. We also conducted an on-line survey of a convenient sample of 60 university program students. To create space for dialogue and interpretation, we facilitated three engagement workshops with key informants who agreed to help us interpret our findings and identify alternative ways philanthropy can be leveraged to support an effective, diverse and equitable cybersecurity field. Finally, we convened an advisory of two seasoned evaluators working at the forefront of equitable practice. Monthly meetings with these advisors helped us to pressure test our approach, identify our own blind spots and assumptions, and identify key areas for continued learning for evaluators interested in how to improve this evolving practice.[10]

We note three relevant limitations to the evaluation and its findings. First, as with all qualitative methods, our findings are not generalizable to a larger group of people or programs. Any of our propositions would need to be tested with other audiences to see if they resonate beyond this group of stakeholders. Second, we used interviews and available information on the programs to describe the cyber programs with which we engaged. While we validated our understandings and landscape with university key informants, our data are necessarily limited and we may have missed important details or mis-characterized programs unintentionally. Finally, both central topics of our evaluation – cyber education and equity – are complex issues. While we have made trade-offs about how to represent what we learned and communicate the findings of our assessment, we recognize that both of these topics are worthy of their own independent investigation.

Organization of the report

The report is organized into sections as follows:

- **The Introduction** describes the background of the Cyber Initiative and the purpose, audience and design of the evaluation.
- **Responding to the Cyber Threat: Hewlett's Approach** provides a brief overview of the workforce shortage issues in the sector and how Hewlett responded and focused on the talent pipeline.
- **Evaluation Findings** are presented in the subsequent three sections, organized by the foundation's three major evaluation questions: where are we now, how did we get here, and where do we go now?
- **Appendices** provide a description of the grants Hewlett provided; the names and affiliations of the evaluation sample; case studies on promising practices used by university programs; a list of programs and initiatives we learned about that might be helpful for foundations to consider; an analysis of the Hewlett team's implementation markers and measurement system; and references.

II RESPONDING TO THE CYBER THREAT: HEWLETT'S APPROACH

The cybersecurity context 2013-2020

Although cyber threats have been present since the 1970s, they proliferated in the 1990s as computer use became more widespread and increasing amounts of data were housed online. In the 2000s the number of known viruses grew by an order of magnitude and attacks became more sharply targeted. Cybersecurity

[10] Our advisory included Julia Coffman, Director, Center for Evaluation Innovation; and Pilar Mendoza, Senior Consultant, Engage R+D.

threats reached a high point in the following decade, with a series of high-profile hacks of national agencies, corporations and society writ large.[11] Key examples include Edward Snowden's 2013 release of highly classified information from the National Security Agency; the 2015 Chinese breach of the US Office of Personnel Management; the Russian-sponsored Wikileaks hack during the 2016 election and the 2018 Iranian attack of 144 US universities.

The US government increased its defensive and eventually offensive capabilities to respond to these growing cyber threats with new arms of the Departments of Homeland Security (DHS) and Defense. In 2004 the Joint Chief's annual National Military Strategy identified cyber as a military domain that must be secured, in addition to the traditional domains of air, sea, land, and space.[12] In 2007, DHS formed the National Protection and Programs Directorate (later rechristened CISA, or the U.S. Cybersecurity and Infrastructure Agency).[13] And in 2009 the government established the Cyber Command at the Department of Defense.[14] These new agencies and efforts centralized the government's siloed cyber efforts under the structure of its defense apparatus, representing the growing prioritization of cyber threats on the country's national security agenda.

A key challenge government agencies faced was how to identify people with the right skills and knowledge to employ in these new departments and teams. The resulting workforce gap was identified formally by the CSIS Cybersecurity Commission, created to provide President Obama with policy recommendations to secure cyberspace. Their 2010 report, *A Human Capital Crisis in Cybersecurity*, summarizes the situation:

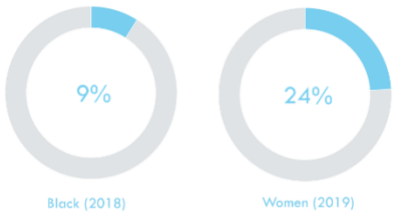
> *"While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills, and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the federal Government or private sector … nor is there an adequately established federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically skilled and cyber-savvy workforce and an effective pipeline of future employees."*[15]

There continues to be concern in government and industry that the current education system is not equal to the task of closing the cyber workforce gap.[16] Government and civil society organizations have begun to address this challenge by advocating for competency-based training and recruitment. The National Initiative for Cybersecurity Education - or NICE - framework catalogues the skills required for roles within the cyber sector to help drive targeted recruitment and development.[17] And in 2018, the Aspen Cybersecurity Group formally recommended that college degrees be removed as prerequisites for jobs in the sector.[18] The government-led Solarium Commission's *Growing a Stronger Cyber Workforce* reinforced

[11] George Mutune, "The Quick and Dirty History of Cybersecurity," *CyberExperts.com*, July 21, 2019.
[12] Chairman of the Joint Chiefs of Staff, "The National Military Strategy of the United States of America," Washington, DC: Joint Chiefs of Staff, 2004.
[13] "National Protection and Programs Directorate (NPPD) at a Glance", *Cybersecurity & Infrastructure Security Agency*.
[14] "U.S. Cyber Command History." *U.S. Cyber Command*.
[15] Karen Evans, Franklin Reeder, "A Human Capital Crisis in Cybersecurity", *Center for Strategic and International Studies,* November, 2010.
[16] A 2018 report on growing the national cyber workforce stated that "employers increasingly are concerned about the relevance of cybersecurity-related education programs in meeting the needs of their organizations"; and a survey of employers by CSIS 2016 found that "only 23 percent thought education programs were fully preparing students to enter the cybersecurity industry" due to lack of practical expertise. U. S. Department of Commerce and U. S. Department of Homeland Security, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future," 52 – 52, May 30, 2018. Evans and Reeder, "A Human Capital Crisis in Cybersecurity"*, Center for Strategic and International Studies,* 2016.
[17] "NICE Framework Resource Center." *NIST*.
[18] Aspen Cybersecurity Group, "Principles for Growing and Sustaining the Nation's Cybersecurity Workforce," *The Aspen Institute,* November 8, 2018.

this move, calling for the classification, upskilling and recruiting of workers from a broad array of educational backgrounds.[19]

Figure 1: Cyber Workforce Participation



A significant diversity gap in the cybersecurity field has also received attention over the last several years. The gap was identified as a priority by the Secretaries of Commerce and Homeland Security in 2018.[20] Recent surveys on the demographic balance in the sector concluded that 24% of cyber jobs were held by women, and 9% by Black people. They also found that Black people and women are overly concentrated in non-management roles when compared to peers with equivalent or less education.[21] 2020 brought increased media coverage of the racial imbalance in cyber and new discussions in leading conferences and fora. For instance, CISA devoted the third day of its annual summit to diversity in September 2020.[22] Particularly relevant in these recent discussions is the frequent argument that homogeneity is in fact counterproductive to cybersecurity. Microsoft's Director of Cybersecurity Strategy for Europe captured this diversity-as-security view, describing that "cyber-attackers are endlessly inventive when it comes to how they break into IT systems. For our defensive capabilities to stay ahead, we need to be even more creative and diverse in our ways of thinking. That can be hard if everyone on the defensive side comes from the same cookie-cutter background."[23]

Opinion pieces in the Washington Post and Forbes are examples of this view gaining momentum.

> *"[There is a] mounting concern that the lack of diversity among cybersecurity pros is hampering the industry's response to serious problems such as racial bias in facial recognition technology and disinformation campaigns that target minorities or are aimed at sowing racial divisions."*[24]

> *"Diversifying the talent pool will provide the opportunity to bring on a wider range of ideas, backgrounds and creative minds onto your team. In a space which is all about outthinking your opponent, a greater range of nationalities, genders and economic backgrounds means more ideas and better defense."*[25]

Hewlett's cyber talent pipeline strategy

The evolution of the Hewlett Foundation's Talent Pipeline strategy occurred during this same period of time, from 2014 through 2020. Among the most significant milestones to date are Hewlett's 2014 granting of $45 million to three anchor university programs; the team's 2017 decision to narrow the strategy's focus to fewer objectives including the development of a policy talent pipeline; and its evolving approach to diversify the grantee portfolio.

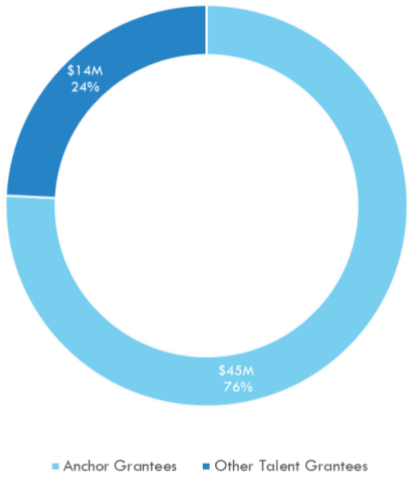
---

[19] Senator Angus King, Representative Mike Gallagher, "Cyberspace Solarium Commission White Paper #3: Growing a Stronger Federal Cyber Workforce", *Cyberspace Solarium Commission,* September 4, 2020.
[20] U. S. Department of Commerce and U. S. Department of Homeland Security. "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future," 52 – 52, May 30, 2018.
[21] We use the terminology Black intentionally here. People of color more generally are proportionally represented in the cyber workforce, largely driven by high rates of Asian participation, while Black participation is low.
[22] "Cybersummit 2020 Day Three: Diversity in Cybersecurity", *Cybersecurity and Infrastructure Security Agency,* 2020.
[23] Sian John, "Why We Need More Diversity in Cybersecurity," *Microsoft News Centre Europe.* May 28, 2020.
[24] Joseph Marks, "The Cybersecurity 202: DHS Is Highlighting Diversity as a Key Cybersecurity Goal", *The Washington Post*, September 29, 2020.
[25] Hadley, James. "To Help Tackle Workforce Shortage, Cybersecurity Needs to Address Unconscious Bias In Hiring", *Forbes,* August 6, 2020

2014 Anchor Grantees

In November 2014, just a few months after the launch of the Initiative, an unexpected release of additional funding allowed the Cyber team to supplement its initial budget with $45 million. The team gave three $15 million grants to enable the University of California in Berkeley, Stanford, and MIT to establish new multidisciplinary cyber centers. Faced with the need to make a quick decision about how best to spend the money, Kramer decided to focus on these universities in part because they were the "obvious choice – they had the greatest strengths across an array of disciplines that mattered for Cyber….I thought to myself, we could really kick this Cyber Initiative off if we did these three grants."

Figure 2: Talent Pipeline Funding

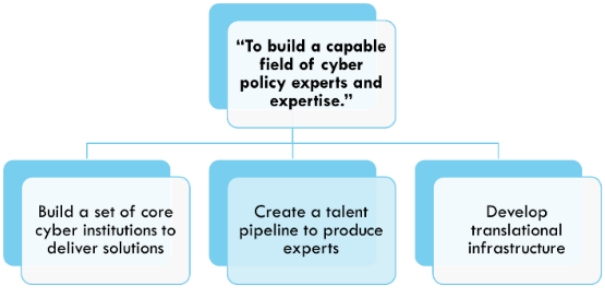


Internal Hewlett documents signal the team's focus on the anchor grantees. As Sugarman described in a 2016 memo to the Board, "our three anchor grantees remain critical to our success, especially the education of new translators and connectors. The importance of those cross-functional individuals make sense and I hope that the new educational programs being developed by the three universities will – over time – develop new talent in this area." When asked to describe the grantees of the university-based pipeline portfolio, Sugarman responds that "there are the anchor grantees and everyone else." Figure 2 illustrates the difference in aggregate funding between these two groups; as of September 2020, anchor grantees have received 76% of the $59 million spent on domestic university grantees.

2015-2017 A Refined Focus on the Talent Pipeline

The Hewlett team has revised the Cyber strategy two times since its launch. In 2015, with Sugarman's arrival, the team organized the strategy around 5 objectives. The team commissioned a 2016 evaluation that recommended a tighter focus and fewer priorities, encouraging Hewlett to consolidate and "narrow to the levers and organizations that are highest performing," or risk losing already made progress.[26] Responding to this feedback, the Hewlett team redesigned its plan to focus on three objectives and advocated to the Board for additional money and time. In 2017, the Cyber Initiative was extended to 2023 and the total budget was increased from its original $65 million to $132 million. The revised goals of the initiative are presented in Figure 3.[27]

Figure 3: Cyber Initiative Objectives



[26] "Evaluation of Network Building: Grants and Beyond-Grant Activities", *Camber Collective,* 2016.
[27] "Cyber Initiative Grantmaking Strategy", *Hewlett Foundation,* 2017.

This juncture also solidified the team's prioritization of the talent pipeline as the largest portion of the strategy.

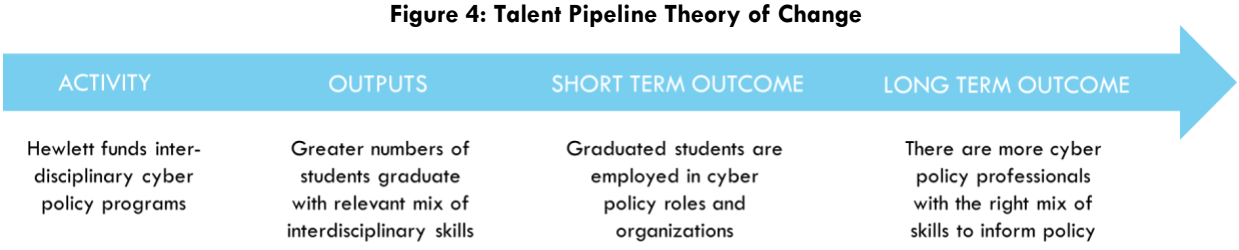
> *"An obvious requirement to build and sustain strong institutions is a pipeline of talented people to work in them. To that end, we make grants to promote the education of experts who have an appropriate mix of technical, policy, and other relevant skills and knowledge. As the cyber field is new and inherently multidisciplinary, this requires innovative curricula and new forms of training. Many fields are potentially relevant: not just computer science and public policy, but also law, business, psychology, sociology, and more. We do not require any specific mix or pedagogical approach, but rather invite universities and other educational institutions to develop their own solutions."*[28]

The premise of the Talent Pipeline portfolio strategy is that increasing the number of people with the right mix of knowledge and skills to advise policy makers on cyber issues requires a new education pathway. It is important to note that Hewlett did not define the problem to solve as the larger cyber workforce shortage, but instead the paucity of national and corporate policy experts who have an appropriate mix of technical, policy, and other relevant skills and knowledge. Hewlett understands "cyber policy" broadly to include not only traditional notions of computer and information security, but also the full range of related policy issues, such as internet governance, net neutrality, encryption, surveillance, and privacy. The Hewlett team decided multidisciplinary cyber education programs were the right target to develop this pathway but that the universities themselves needed a push: "there was demand from employers for these people [and skills], but universities were not answering," explains Sugarman. "Someone needed to be the first mover."

As part of the evaluation process, we validated with the Cyber team the Talent Pipeline theory of change and its underlying assumptions. Represented in Figure 4, the theory of change reflects the team's belief that an increase in university-based interdisciplinary programs would help fill the gap in the cyber policy workforce with professionals with the right mix of skills and knowledge. Three key assumptions underly this logic.

- The problem Hewlett can help solve to address the shortage of cyber policy talent is the lack of a sufficient number of interdisciplinary university programs.
- If there are more university cyber programs, there will be an increase in the number of people working in policy jobs and able to advise decision makers.
- If elite universities start multidisciplinary cyber programs, it will lead to competition and the creation of additional multidisciplinary programs as institutions respond to market forces and student demand.

Figure 4: Talent Pipeline Theory of Change



[28] Ibid.

Interested in creating a cyber policy field that is "robust, high quality and enduring," Hewlett's approach was to learn what might work, rather than prescribe to grantees certain programmatic components the foundation needed to see. Over time, the team paid attention to the strength of the curriculum and instruction offered, faculty appointments targeted at cyber policy research and education, placement of students after graduation, and program financial sustainability. These elements became the measures – or implementation markers – the foundation used to track the progress of the portfolio through annual surveys of their grantee partners.

Table 2: Talent Pipeline Implementation Markers

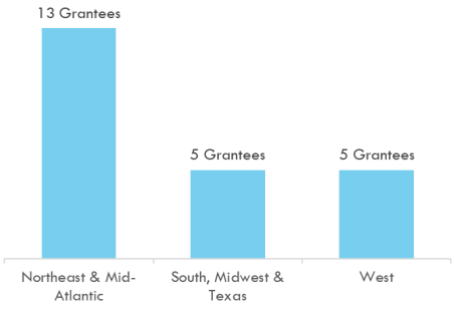
Implementation Marker	Description
Curriculum maturity	Grantees are making substantial progress towards establishing an interdisciplinary cyber program including courses, modules, or degrees
Diverse & accomplished staff	Grantees' faculty, staff, fellows, etc. are increasingly inter-disciplinary, and new positions are filled quickly
Student outcomes	Graduates enter the cyber policy field in positions across industry types
Diversified funding	Hewlett making up a smaller YoY% of budget; and hiring non-policy staff
Response to cyber debates	Grantees are amongst the leading responders proposing viable solutions to 3 or more of the "top 5" cyber debates/events each year
Relevant research	Grantees' research is rigorous, peer-reviewed, and relevant, advancing key debates within the field and informing decision-makers

We refer to some of these markers in our findings. (We analyze their progress and identify challenges with the measurement system the Hewlett team used to track the markers in Appendix V.)

2019-2020 An Evolving Approach to Diversity

The Cyber team's pursuit of diversity goals is a third thread in the team's strategic journey. In 2019, Hewlett made two new grants to George Mason and University of Indiana to "serve students from different geographies and communities who have different policy viewpoints." The geographical diversity of the current portfolio of grants is represented in Figure 5.

Figure 5: Grantee Geographic Distribution



Sugarman identifies these two grants and additional investments to schools in the middle of the country as representing the team's approach to diversity after the 2017 strategy refinement. "Our grants focused more overtly on gender, geographic and viewpoint diversity.[29] We have not made as much progress funding schools that have significant populations of minorities and people of color." When asked why this was the case, Sugarman describes the foundation's approach to identify potential grantees:

> "None of these programs existed when we started funding them; we had to create all of this… We identified a class or a leading expert with a class… They came to us or we sought them out… Key was the individual with the vision or authority to develop the program… We had to find leadership and programs that we were totally comfortable with…."

Sugarman goes on to say that the team was not interested in purely technical programs, or those led by faculty members who lacked the university backing, vision or sufficiently "impressive government, private sector or academic accomplishments."

[29] 9 of the 23 grantees in the portfolio are led by female faculty.

The 2020 racial movement motivated the team to think differently about diversity. In a team memo to the Hewlett board, Sugarman explains: "in light of the clear need for greater racial diversity in the field, we plan to explore grants to other institutions serving racially diverse student communities." This evaluation was commissioned in part to help the team pursue this goal and "draw out how well our university grantees are or are not serving communities of color and other historically underrepresented groups. The evaluation will help identify concrete steps we can take to overcome whatever obstacles exist to bringing more people of color into the field."

III WHERE ARE WE NOW?

Ultimately, data on program enrollment, student completion and employment will be important to any summative effort to measure whether the cyber education programs Hewlett funded are in fact producing the experts Hewlett expects to see result from their investments. While the Cyber team's measurement system collects data on the sectors in which students take their first job, many programs are new and do not track sufficient enrollment and completion data; others do not keep track of student employment. An on-line survey of a convenient sample of 60 university program students – both Hewlett grantee and non-grantee – revealed that 90% of students are largely satisfied with their participation in these programs, though 49% of respondents identified job placement as a key gap in the services they receive.[30]

With the limits of student completion and placement data in mind and in response to the Hewlett team's ask for a map of cyber programs, we answer the first evaluation question by developing a taxonomy that helps us compare Hewlett-funded cyber programs to non-Hewlett programs according to three dimensions: interdisciplinarity; formality; and prioritization of diversity, equity and inclusion. We chose these factors to drive our landscaping because of the Cyber team's interest in multidisciplinary education; its hope to support enduring programs; and its commitment to understand how best to improve diversity, equity and inclusion.

Figure 6: Student survey results

In an online survey of 60 cyber program students and recent graduates – from both Hewlett grantee and non-grantee universities – we found that:

- 80% identified faculty as the biggest strength of their program; 65% identified the curricula.
- 90% would choose their program again.
- 49% want additional support from the program for their job search.
- 86% feel prepared for their preferred job following graduation.
- 70% had access to experiential learning opportunities.
- 19% reported facing equity-related challenges in their program. 47% of responders self- identified as people of color and 41% self-identified as female or other.

The Hewlett grantee portfolio

The number of universities with cybersecurity programs has increased over the course of the last decade. As of this year, there are at least 188 US universities that offer master's programs in cybersecurity – this number does not include higher degrees, bachelor's degrees or certificate programs that are also available.[31]

Universities take different approaches to cyber education. As a technical discipline, cybersecurity traditionally includes a core curriculum that contains aspects of computer science, networking,

[30] This sample comprises 60 students across 7 grantee universities and 3 non-grantee universities. We selected this sample by offering all programs the option to share the survey with their students. The students that completed the survey were 51% white, 22% Asian, 22% Hispanic, 9% Black, 2% Native American, and 2% Pacific Islander.

[31] Steve Morgan, "2021 Directory of M.S. In Cybersecurity Programs at Universities in The U.S.", *Cybercrime Magazine,* January 11, 2021.

cryptography, and hacking. The Hewlett team targeted university programs that deliberately combine technical knowledge and skills with disciplines like political science, business and law.

The domestic university programs that have received Hewlett grants all feature this interdisciplinarity. True to Hewlett's intention to learn about different models, grantee programs vary according to whether they are in public or private universities; which specific disciplines they marry; if they include experiential initiatives for students; and whether they are housed in a policy, law, computer or social science department or policy school.

The amount of money and focus of the grants Hewlett provided these programs also varies. While most of the grants were for academic education programs, over one third were not. Grants to Georgia Tech and the Harvard University Belfer Center fund research programs or projects. Temple University's funded program is a multi-day cyber technology boot camp for policy makers to be held in Spain, and Cal Poly's grant supported cyber training courses to employees of private companies and state government. The grant to Penn State University was for a new open access cyber textbook. Grants to Middlebury and the University of Maryland funded short-term cyber workshops. The grant to Yale supported one class rather than a full program.[32] (The full list of universities and grant purposes and amounts are included in Appendix I.)

A map of cyber programs

There was wide agreement across all our interviews and workshops about the value that interdisciplinary knowledge and skills bring to the cyber field. The heart of the reason is that cyber threats and issues are technical in nature, but require a deep understanding of policy, business, law and human behavior to resolve and build preventive capacity for the future. It is not only that cyber teams need to include experts with diverse skills, but also that individual professionals need to be able to translate between relevant disciplines. "Interdisciplinary education," explained a key informant, "helps students ask and answer questions differently, frame the world in new ways…. Interdisciplinarity makes for a safer and more secure cyber space."

Universities offer classes with cyber relevant topics in many disciplines. While some programs offer cyber-focused classes in their computer science, law, political science, policy or engineering departments or schools respectively, others pursue a deliberate marriage of disciplines in new curricula offered to students across schools and departments. We capture this variation in Figure 7.

Figure 7: Taxonomy - Interdisciplinarity

Given Hewlett's emphasis on multidisciplinary education and training, we used this taxonomy as a proxy to measure the degree to which students are actually taking interdisciplinary classes and receiving an interdisciplinary education across technical and non-technical disciplines. In other words, a school may offer cyber-related courses for both its computer science and policy students respectively, but the fact that both of these are *offered* does not mean that individual students are in fact taking classes across disciplines, and thus gaining multidisciplinary knowledge and skills. We define the creation and implementation of new, interdisciplinary curricula that educate students in this way as "full" interdisciplinary education programs.

[32] To note, Hewlett's grantee surveys ask grantees to report on the academic cyber programs at their universities rather than on the specific work (program, textbook, class or workshop) that Hewlett funded. This presents a challenge for using these data to measure the progress made by Hewlett grantees, given that the data do not always reflect the activities that Hewlett supported.

Real barriers exist for universities seeking to develop full interdisciplinary programs.
Key informants describe the significant challenge they face going against the grain of discipline-focused norms, incentives and resource allocation. A key informant at an elite university described the experience: "We had hoped to make a degree program but… it's very hard to do a multi-disciplinary degree program here… So far nobody wants to go through the process – capital needs to be spent to push faculty and deans to go along. We had a full-blown proposal about curriculum and there was advocacy internally and lots of conversations with relevant deans. There's always interest but we haven't moved the car. It was taking so much time and it was too difficult to convince the powers that be."

We learned of three specific obstacles that program leaders and advocates face:

Tenure
Because faculty tenure is usually discipline based, interdisciplinary programs are not recognized as part of faculty promotion. Several key informants described the very real constraints of disciplinary knowledge and norms: "any complex problem tends to be approached from narrow disciplinary perspectives because interdisciplinarity is really hard…You are rewarded for excelling within your discipline so there are disincentives for faculty to do it…."

Financial Resources
Several people describe university funding models as a barrier to interdisciplinary education. "There is an eat what you kill mentality; none of the schools want their students to take classes anywhere else, because [departments] lose those funds….so there is potential for a turf battle if I start leaning hard on the interdisciplinary mission of the program."

Tuition sharing initiatives and outside funding can help alleviate internal inertia. Two Hewlett grantees shared their experience that Hewlett's support was integral to helping them overcome barriers and attract university resources. In a grantee's words: "The university had not been behind the effort – there's been skepticism. It wasn't the faculty's baby, so they didn't care about it. Until we achieved self-sufficiency last year, there was reluctance to put resources behind the program. Hewlett was the lynchpin that gave us time to figure out our model and get the university behind us. Now, the office of research and economic development at the university is funding us."

Non-Hewlett grantees' perceptions confirms that funders can be instrumental to helping to incentivize interdisciplinary education. In the words of a non-grantee: "We work together, but programs tend to be fairly isolated. Programs are funded based on attendance of students, which makes sharing hard."

Sponsorship
A consistent theme across all key informants was the role that senior university leadership plays in developing and maintaining effective interdisciplinary education programs. When the provost, president and/or deans are directly involved, they can direct funding, advocate to others the benefits of interdisciplinarity, resolve bureaucratic barriers to work across schools or departments, and marshal resources to hire new faculty. Where this kind of sponsorship does not exist, programs struggle. In the words of a program leader, "to be more united, we would need high-level champions – president or provost or trustees – or donors advocating for it."

Interdisciplinary curricula appear to be more successful when owned by more than one school or department. A promising practice is to institutionalize joint governing bodies comprising leaders who come together to make decisions about the cyber program curriculum. At the University of Indiana, the governance committee brings together the four schools whose deans jointly offer the cyber master's program. At Virginia Tech, an integrated curriculum committee with representatives from the three colleges involved in the cyber minor make joint decisions about the course of study.

The more formal an interdisciplinary program, the more likely it is to endure.
Key informants describe how interdisciplinary programs can be temporary if they are attached to an individual professor or champion and not institutionalized in the form of a major, minor or specific degree. "A formal commitment is important," shared a key informant whose interdisciplinary program was short lasting, "because people change and without formalization there is no guarantee informal interdisciplinary cooperation will continue." We learned of two cyber programs that closed in part because of this lack of formalization.

The Hewlett portfolio as well as our larger sample include programs with varying degrees of formalization. We capture this variation using the taxonomy in Figure 8.

Figure 8: Taxonomy - Formality

As with establishing interdisciplinary education, creating a formal program often requires overcoming bureaucratic obstacles that can take a year or more to surmount depending on the school. Many program leaders decide not to take this path because high transaction costs and organizational politics act as a disincentive for putting in the necessary time and effort: "the university does have the ability to offer certificates," explained one key informant, "but the process is so deeply bureaucratic. We didn't deem it to be worth the effort…. There would be even more bureaucratic costs to a full master's."

Bureaucratic obstacles to formalizing inter-disciplinary cyber programs exist across universities and anchor and non-anchor grantees. "We explored turning our initiative into a degree program, but it is too politically difficult. We developed a curriculum and had internal advocacy and a very senior leader with a three-school appointment and still it did not move forward." One of the foundation's three anchor grantee program leaders shares this same experience, "we do not have a cyber focused education program because of the way the university works. It's not our choice." The lack of leadership commitment to formalizing programs is also evident when curricula development is treated as voluntary work. We heard from several faculty that they develop programs on their own time and are neither financially nor professionally rewarded to work on interdisciplinary education.

10 of 23 domestic university Hewlett Grantees have formalized, interdisciplinary programs.[33]
The map of our sample of grantees (blue) and non-grantee programs (black) across these two dimensions of interdisciplinarity and formality is presented in Figure 9. If we use this as the basis upon which to measure the progress of Hewlett's portfolio, the blue schools in the upper right corner of the chart are those that exhibit the more interdisciplinary, formalized programs.[34]

[33] We do not include Cal Poly in this landscape because it is a training program for professionals, not an academic program for students. We do not include Harvard Belfer because it is a research-based program, not an education-based one. And we do not include the University of Maryland because we were unable to interview the program's leaders.
[34] We define "formalized" to mean a program that offers a certificate, minor, or degree. We define "interdisciplinary" as a program that unites more than one discipline, and offers mostly new, custom classes (rather than existing courses).

Figure 9: Landscape of Cyber Programs

Diversity is vital to cyber policy but inconsistently prioritized in cyber education

When we include diversity, equity and inclusion in our taxonomy, we learn more about the conditions that support change along all three of these dimensions and what lessons these examples might have for other program leaders and universities.

Diverse experience, backgrounds, perspectives and the "ability to think outside the box" are described by both employers and current cyber policy professionals as essential to effective cybersecurity policy and practice. For many of the key informants we met, this means that the racial, ethnic, and gender diversity of cyber teams is imperative for effective cybersecurity and integral to the often described professional competency of being able to anticipate and understand situations from a variety of unique points of view.

Despite this recognition, there is significant variation in how cyber program leaders approach integrating diversity, equity and inclusion in their programs. Among our sample of 38 programs, we identified:

- Program administrators who see the issue largely as one of increasing the number of students who attend their program from diverse racial, ethnic and/or gender backgrounds, and identify the larger university context in which they work as the main constraint (the common refrain we heard was: "if your university is not diverse, the program won't be");
- Program administrators who lead or participate in recently launched efforts or committees conceived to analyze, identify priorities and plan for how best to improve diversity in their organizational contexts;
- Program administrators who prioritized diversity and equity before 2020 and have developed partnerships, initiatives, education formats and business process to increase diversity of students and faculty and include equity topics in their curricula; and
- Program administrators at minority-serving institutions focused on bringing interdisciplinary cyber education and opportunities to student bodies that are primarily non-white.

We represent the variation in these approaches in Figure 10.

Figure 10: Taxonomy – Diversity, Equity, and Inclusion

6 out of 23 Hewlett grantees prioritize DEI in their cyber programs.
In our interviews with university program faculty and leaders, we asked open questions about how individual leaders understand and approach diversity, equity and inclusion or DEI. We did not define the term DEI for them but instead sought to understand their definitions, priorities and any steps they've taken. Some key informants were very candid that they "don't do anything" to integrate DEI principles or priorities in their programs. Others shared relatively recent convenings, planning, meetings and discussions taking place in light of the 2020 social justice movement. Still others developed initiatives before 2020 and are already implementing them to achieve specific results. We define this last group as the set of university programs that prioritize specific DEI action. Examples include efforts to improve the equity of recruitment practices, integrate relevant subject matter into teaching curricula and establish partnerships with Minority Serving Institutions with the specific goal of increasing their student body's access to cyber courses and faculty.

A few illustrative practices are described below, with more details provided in the case studies in Appendix III.

- George Mason's program is designed to be accessible to a broad array of communities. The program partners with Hampton University to offer students specialized ABA-certified training that then allows George Mason to admit them without the need for LSAT scores. George Mason students also participate as mentors to students with other Minority-Serving Institutions. The program lead is currently working to design a partnership with Howard University to experiment with ways to interest more people of color in the intelligence community; and is focused on increasing the proportion of female professors and acting intentionally to recruit Black fellows.

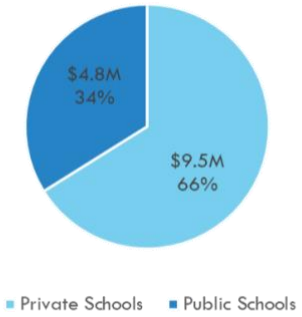
- The cyber program at Virginia Tech offers an interdisciplinary educational experience designed with equity in mind. The school has recently completed the first semester of its new Integrated Security minor, a cross-college program that unites what it calls cyber and "human" education and offers a course of study that spans the colleges of engineering, business, and liberal arts. The program specifically engages with questions of equity in its curriculum – for example, classes will consider issues like the varying access to digital infrastructure different communities enjoy. All of the program's courses were evaluated to ensure they engage with equity issues and questions before the minor was formalized.

- While hosted at a university, San Luis Obispo's Cal Poly California Cybersecurity Institute (CCI) runs a cyber workforce education program that is not part of the university curriculum. Working through industry partners, the CCI helps already-employed professionals to develop cyber skills to become more competitive and/or make a mid-career shift into a cyber-based role. The CCI also operates a statewide and nationwide K-12 program, concentrating on schools in disadvantaged areas catering to diverse students. The program began in 2016 with 40 students and will scale to 20,000 this school year. This year, the CCI plans to launch a pilot project with two California Community Colleges, members of Upskill California, and the California Employment Training Panel to help build out certification training programs with the goal of expanding to the remaining 27 Community Colleges.

Public universities are more likely to prioritize diversity, equity and inclusion in their cyber programs, yet received smaller grants and aggregate funding in the Hewlett portfolio.

Using our taxonomy we note that as of September 2020, 45% of the public school cyber programs in our sample have prioritized specific DEI actions, compared to 28% of the private schools. Although the Hewlett Talent Pipeline portfolio has almost equal numbers of public and private school grantees, private schools received 95% more overall funding than Hewlett's public university grantees (excluding the anchor grants).

Figure 11: Total Grant Funding (Excluding Anchors)



Minority-Serving Institutions Are Excluded from Hewlett's portfolio.

Our sample included cyber-focused faculty at 5 MSIs and 12 people of color now working in cyber policy careers. Throughout interviews and workshop dialogues, we had the opportunity to hear about the successes, opportunities and challenges facing faculty and students at Minority-Serving Institutions.

The faculty with whom we spoke currently run or are working to establish effective cyber programs at their institutions. Entrepreneurial leaders create and attract partnerships with private companies such as Apple, Netflix, Amazon, and Motorola; apply for NSF resources to fund scholarships and stipends; and lead coalitions of universities working with national labs and departments. These leaders recognize the value interdisciplinary curricula and training bring to cyber education but often grapple with the lack of funding and leadership support needed to develop and formalize them. Among the interesting curricula we identified through the evaluation is Norfolk's master's in Cyber Psychology – an interdisciplinary degree that combines computer science and psychology to examine the interplay between deviant digital behavior and underlying psychologies.

Faculty at Minority-Serving Institutions in our sample describe the challenge presented by a lack of absolute resources rather than a lack of administrative practice or department motivation to share resources in order to create interdisciplinary programs. Funding to maintain and grow the program is heavily constrained by the specific challenges associated with bringing in new support to an HBCU with a small budget. In order to build out the program, it is necessary to raise funds to bring in additional faculty. Doing so requires university-level support. However, in a low-budget setting, investment decisions between programs are often made with zero-sum logic: the programs that bring in the most money are more likely to receive additional university investment. Thus, programs that are still in development, and are thus not yet budget-positive for the university, can struggle to receive the institutional support that they need to reach that level of financial maturity. And without robust staffing, they do not have enough capacity to pursue all the available sources of external support that are available. "I have a sense that funders have a "we'll give you money, you make it work" expectation. But the people in the room don't understand the challenges associated with the dynamics of building programs at HBCUs."

Key informants identify Minority-Serving Institutions as a significant opportunity for philanthropy

People of color working in cyber policy in both private and public sectors describe the value and difference that HBCUs make. 5 of the 12 cyber policy professionals of color in our sample attended HBCUs or HSIs (Hispanic Serving Institutions). All of them and most of the rest of our key informant sample identified the opportunity for philanthropy to support interdisciplinary cyber education where the students and faculty are already diverse, rather than targeting predominantly white universities and then encouraging them to prioritize DEI. Many of our key informants - across universities, employers and DEI experts – emphasized and supported this point, noting that funders "need to go to where people are,

where they're comfortable, where their community is."[35] The literature supports the view that MSIs offer a community of learning where students of color are in the majority and an atmosphere of equity is maintained; a recent paper notes that "an important feature of HBCUs has been their provision of a welcoming environment for black students, who are able to thrive in a context of acceptance and mutual support."[36]

IV HOW DID WE GET HERE?

The Hewlett Foundation's Cyber Talent Pipeline portfolio was developed to launch multidisciplinary cyber programs and create models of training and education to increase the number of people employed to advise forward looking, complex cyber policy. Now more than 6 years later, the foundation has seeded and supported a rich variety of university-based cyber programs and efforts. The Hewlett Foundation's lack of prescriptive guidance to grantees allowed program leaders to meet the constraints and opportunities presented by their respective university contexts. We learned that the university context matters significantly; the nature of leadership support, funding, discipline embeddedness and cross-department collaboration can shape the degree to which programs develop interdisciplinary curricula that are likely to last because they are manifest in formal degree programs.

Diversifying cyber education or making the field itself more diverse, equitable and inclusive were not part of the strategy when it was first developed.[37] In 2020, the cyber team made explicit its desire to learn more about the progress, obstacles and opportunities to taking a more deliberate approach to this revised goal in the Talent Pipeline strategy. The assumptions underpinning the Talent Pipeline strategy from 2013-2020 centered on the idea that university-based cyber programs can increase the number and quality of cyber policy experts and thereby close an important gap in the cyber workforce. A focus on equity encourages a sharper questioning of underlying assumptions to highlight the structural barriers to access facing many people who cannot attend universities in the first place.

In this section, we seek to inform the foundation's reflections by introducing the heart of the insights we gained by applying the principles of the Equitable Evaluation Framework (EEF). We share what we learned about the weight of philanthropic concepts and going-in assumptions; and the perception that inequity and access are relevant for all fields, no matter how nascent. We build on these insights by presenting two co-created strategic frameworks that form the basis of our final findings and recommendations about how Hewlett and other funders can best leverage philanthropy to support an effective, diverse and equitable cyber field moving forward.

[35] Of interest is a recent Washington Post article by Nitasha Tiku on the opportunity private companies have to strengthen the equity of their recruitment practices vis-à-vis HBCUs. See "Google's Approach to Historically Black Schools Helps Explain Why There are Few Black Engineers in Big Tech," March 4, 2021.

[36] Earnest N. Bracey "The Significance of Historically Black Colleges and Universities (HBCUs) in the 21st Century: Will Such Institutions of Higher Learning Survive?" *American Journal of Economics and Sociology* 76, no. 3, 670–96, 2017.

[37] In 2019, the team expressed an intention to fund DEI-focused organizational effectiveness grants, share best practices related to diverse hiring and other DEI efforts, prioritize discussion of diversity in grantee conversations, and encourage grantees to improve their DEI policies.

A philanthropic strategy based on a pipeline concept assumes away barriers to access.

One of the strongest points of feedback we heard in our interviews and workshop discussions was that the *pipeline* concept that motivates Hewlett's grant giving is inherently biased because it assumes away differences in people's experience of barriers to access to social, economic and educational resources. More specifically, the assumption that all that needs to happen is to add more programs, so you can add more people to attend and graduate with the right knowledge and skills to get the right jobs, misses the structural inequity people face with respect to money, education and employment.

The figure to the left identifies barriers to access that came up in our interviews and workshops. In the words of one of the many key informants who shared this view:

"You can't just put people in a pipeline and expect the outcome will occur…It just doesn't work like that… If you're not in the pipeline, you don't get access to opportunities along the pipeline."

Our key informants identified three major challenges to the foundation's strategic framing.

First, a talent pipeline concept assumes that people face equal opportunities to identify cyber as a viable career path when the reality is that socioeconomic barriers prevent many people of color from choosing a cyber career. In fact, it is more likely the case that a lack of financial resources leads people to choose different paths to work and education. Families can lack the money to buy computers while students are in middle and high school; to support training so students can get entry level roles after high school; and to pay for enrollment in those universities that have cyber programs.

Social networks were identified as equally important barriers to accessing a cyber education "pipeline." We heard from many of our key informants that there is a "failure of imagination" that can result from the reality that cyber is not promoted early enough or in the right places to help more people imagine a future that involves cyber. As one key informant explained, "you can't visualize a path for yourself that you don't know about."

People's direct comments help illustrate this point.

> *"The messaging around opportunities to join the cyber field is not happening where black and brown people are… at their schools and at the places and platforms where they consume media."*

> *"A large blind spot is the belief that the people who are interested in these careers know how to get there, and if they don't pursue the degrees it's because they are not interested. The problem is that the messaging about these career paths is not in the places where people are."*

"Lack of access to networks and mentors has set me back in ways I'll never be able to quantify. I am a first generation American, and I didn't have a person to call to ask what classes to take, to point me towards certain directions or careers.

"There's a legacy of communities who have been deliberately excluded from these technical careers - told in high school they're not suited for them, wouldn't like them, aren't smart enough for them. Told that if they can't code they can't get a role in cyber - which is just not the truth."

Second, a cyber talent strategy that invests in university programs as the starting point of its pipeline misses the reality that people can take diverse pathways to a cyber career and a cyber policy role within it. We heard from people of color who had entered the cyber field through training and apprenticeship programs and then went on to move into higher level and policy-oriented roles once employed. We heard from people who run apprenticeship programs and work with companies and government agencies to place graduates upon their completion. We heard from people who started in the military, excelled at technology-based pursuits and eventually joined policy focused agencies and/or teams. By engaging DEI experts working in cyber, we were reminded that the 2018 Aspen report "*Principles of Growing and Sustaining the Nation's Cybersecurity Workforce* " recommended removing college education as a requirement for cyber jobs as progress in diversifying the field; and that mid-career women, military vets and other professionals who do not already work in cyber can benefit from affinity groups that provide opportunities to network, identify mentors and allies within the industry.

Third, the foundation's assumption that completing a cyber interdisciplinary university program will lead to employment in cyber policy neutralizes the inequity experienced by many people of color and women who face high barriers to promotion and retention once they get a job. "People often become policy people over time," explains a senior cyber policy professional in the private sector, "most people don't go straight into policy roles. They become policy people… You need to have some road under you before you're looking at policy roles."

This presents another challenge as once people of color and women get into the industry, they can face disproportionate barriers to promotion and retention. "There's a real lack of women at a leadership level," shared a women of color who works as a cyber policy expert and is the only woman and person of color on an executive team. "Women drop off. They don't feel comfortable and don't aspire to these levels because it's not comfortable. You always feel and are made to feel the imposter syndrome… I am often underestimated because people find it incongruent to look at me and see someone with a long career in national security and cyber."

Other people of color and advocates working to improve networking through affinity groups shared their views on this phenomenon: "If you don't see people in the middle or senior level, you feel like you can't get there. And when you have negative or oppressive experiences, you internalize them through that lens and recognize in a very personal way that this space was not created for you."

The assumption that elite universities are best placed to enable multidisciplinary cyber education is not borne out by our evidence.

Hewlett's timely, forward looking transition from nuclear to cyber policy spurred the initiative and led to a relatively large funding portfolio to seed and support program development at 23 domestic universities. Through our interviews with Hewlett staff, we learned of the unpredictable administrative change that required the team to make a quick decision about how to spend $45 million in the first few months of the strategy. Hewlett colleagues characterize the decision to give $15 million grants to three "anchor" universities as a reflection of the trust the team and Board have in these institutions given their capacities and ongoing relationship with the foundation.

External stakeholders perceive this relationship to be contradictory to the notion of building a field. "Hewlett's reflexive move," shared one key informant, "is to give millions of dollars to elite institutions that are incredibly problematic institutions from a diversity point of view. Other organizations are much more deliberate."

Using our taxonomy, we did not find evidence that the anchor schools demonstrate a difference in progress commensurate with the higher amounts of funds they received from Hewlett. The inclusion of a wider sample of programs allowed us to understand variation and conditions that drive more interdisciplinary education and formalized programs. It is worth underscoring that creating new programs that prioritize education across disciplines does not come naturally in many university contexts; deeply embedded discipline-based norms and bureaucratic barriers to change can obstruct creativity and innovation.

We did find evidence that one of the anchor universities in the Hewlett portfolio has launched a new school, supporting Hewlett's expectation that its financial support could motivate additional program development to meet student demand. At MIT the initiative that Hewlett funded is described as the "leading model" for what now is a new college of computing that reorganizes how the school approaches research and education in computer science and other disciplines. "We are now part of that college, explains one of the MIT program faculty, "which was one of the goals the foundation shared when they gave these grants; their money would be the angel investment to kick things off, and the university would then put up money to keep it going….We will be hiring 50 new faculty members over the next 5 years. This is the largest expansion in MIT faculty since the Sloan School was created in the 50s. It will have 3 missions – to be great at computer science; to promote cross-disciplinary research and education…. and to address the social, ethical, and public policy impact of computing."

The Hewlett strategy development process may need new tools and processes to integrate the foundation's commitment to diversity, equity and inclusion more fully.

The Hewlett Foundation's commitment to diversity, equity and inclusion was first published in 2018 in a post written by Larry Kramer.[38] In 2020, the foundation reemphasized its commitment to the "importance of diversity, equity, and inclusion both internally, in our hiring process and organizational culture, and externally, in our grantmaking and related practices."

The 2020 statement explains the foundation's perspective:

> "We have a duty to exercise this privilege—for it is a privilege—thoughtfully, mindful of the larger society of which we are part, and of the historical, economic, and cultural forces that shape it. We believe this duty includes a responsibility, in hiring staff and choosing grantees and other partners, to recognize that some groups have been historically disadvantaged, whether by virtue of race, ethnicity, socioeconomic status, gender identity, sexual orientation, ideology, religion, or other characteristics that reflect significant social categories or fractures. While our efforts encompass a wide range of identities, we believe the unique history of racial injustice in the United States imposes a special responsibility to make intentional efforts to address systemic racism, both internally and in our grantmaking."[39]

The foundation's DEI commitment mirrors the perspectives we heard about the opportunity Hewlett and other funders have to identify and consider structural inequities that prevent people from pursuing cyber careers. The evolution of the Cyber Initiative suggests opportunities where these principles could have been integrated sooner and consistent with the sector's 2018 analyses on the racial diversity gap. In retrospect, we see a blind-spot associated with the team's aspiration to solve for

[38] Larry Kramer, "Committing to Diversity, Equity and Inclusion," *Hewlett Foundation,* January 2018.
[39] "Diversity, Equity and Inclusion." *Hewlett Foundation.*

the lack of a certain capacity in a field by building a talent pipeline that goes from universities to employment without referring to the people that do and do not have access to this university pipeline in the first place.

There are opportunities to improve the rigor of the foundation's strategy development process to sharpen problem and assumption definition, listen to people across different domains and develop strategic concepts that reflect real differences in people's access to privilege.

We provide here three recommendations for how Hewlett teams might adjust their strategy development and review processes with this learning in mind. These include:

1) The opportunity to include in strategy development sharper problem definition and landscaping analyses that explicitly analyze how people with different backgrounds and experience are impacted by the current state in a specific area;

2) A more rigorous process for teams to specify and document underlying assumptions about who is served by a particular strategy early on in the strategy development process;

3) An expectation that teams seek feedback from a diverse group of stakeholders on their core strategic concepts and assumptions to identify unintentional blind spots before the lion's share of grant dollars are dispersed and with some regularity over the course of a strategy's lifecycle.[40]

V WHERE DO WE GO NOW?

In this section, we present recommendations for the Hewlett team to consider as it plans for the remaining two years of the Cyber Initiative; and recommendations other funders might consider when thinking of ways to contribute to an effective, diverse, equitable and inclusive cybersecurity field.

Recommendations for Hewlett:
Fill gaps in the portfolio before exiting the cyber field in 2023

With an eye on the remaining budget, the size of Hewlett's team and its existing portfolio of grantees, we build on our findings to present four recommendations for the Cyber team to consider.

1. ***Double down on public universities already in the portfolio.***
   Given what we learned about the difference between public and private universities, and the diverse trajectories people take to pursue career paths, there is a compelling case to be made for Hewlett to identify and help fill the gaps faced by public universities already in or new to the Cyber portfolio. The Cyber team might use the taxonomy to co-create proposals that help university grantees move toward more formalized and therefore enduring programs. The foundation's cache and social capital might help persuade the highest level of these universities to support and commit to the programs if university support remains a gap to fill.

2. ***Support schools where the student population is predominantly non-white to help create the conditions for robust cyber programs.*** This was one of the top two recommendations we heard from all our key informants. Community colleges and Minority-Serving Institutions are more likely to have predominantly non-white student bodies and faculty. We heard from many key informants about the lasting impact and tremendous value that HBCUs bring to students. We

[40] The Hewlett-led Listening innovation could be a helpful, actionable source of feedback in the strategy development process. See Fay Twersky, "The Listening Post", *Hewlett Foundation,* November 2, 2020.

identified 5 Minority-Serving Institutions to be in our evaluation sample; each has committed Cyber faculty, existing innovative partnerships and the opportunity to further develop interdisciplinary education programs. We learned that Cal State San Bernardino leads a national collaboration of more than 300 universities and colleges dedicated to cyber and piloting innovations, many of which are community colleges. The Cyber team might engage with these types of leaders to identify projects that face gaps in funding or sponsorship, where philanthropic monies and social capital can be leveraged to take innovative curricula or approaches to diversify cyber to scale or influence leadership support for cyber programs.

3. ***Invest in HBCU partnership models, reversing the power dynamic by granting to the HBCUs***. Carnegie Mellon and George Mason have developed partnerships with HBCUs, intended to increase student enrollment in universities with already established interdisciplinary cyber programs. Partnerships ongoing between some of these universities and predominantly white partners tend to grant philanthropic resources to the latter. We heard clear feedback that these partnerships are valuable, but that the resources would be leveraged more and the signaling more constructive if the HBCUs could receive the money and choose their partners rather than the other way around. The Cyber team might use its resources to support additional partnerships, granting to the Minority-Serving Institution and giving them the flexibility to decide with which other school to partner to increase student access to cyber faculty, networking and other opportunities of common interest.

4. ***Replicate the NSF award.*** Several university program leaders, employers and cyber professionals told us about the National Science Foundation's CyberCorps or Scholarships for Service program – a nationally funded program to recruit and train cybersecurity professionals by providing scholarships and stipends for undergraduate or graduate education. Given the financial barriers facing many people who want to pursue university programs, the Cyber team might replicate this program and tailor its resources to women and/or people of color interested in cyber education and professional paths.

5. ***Support, document and share the models used by those cyber programs that reach high degrees of formality, interdisciplinarity and DEI prioritization.*** Many program leaders with whom we spoke shared both an interest and desire to learn from peers across the country. The Cyber team might add to its current portfolio an effort to convene these programs, document and publish their lessons learned and use its voice to advocate for others to fund these models and in particular their ability to implement DEI initiatives with concrete outcomes for students.

Recommendations to other foundations:
Address barriers to access to help create a diverse, equitable cybersecurity field

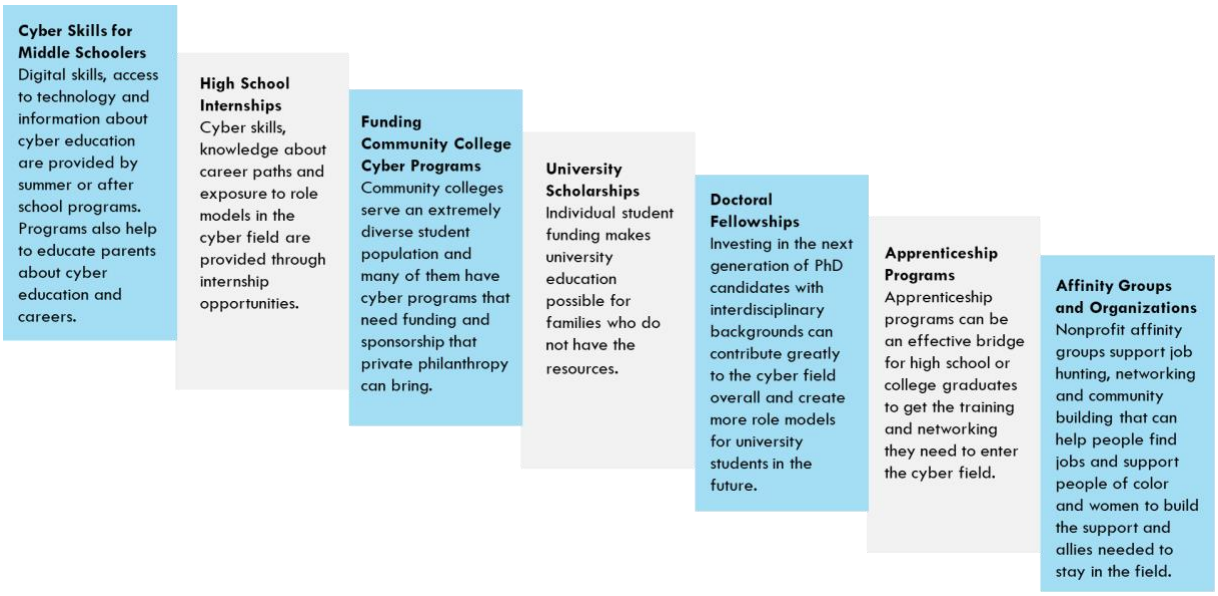
For foundations interested in complementing Hewlett's investment in university cyber programs, we suggest considering the challenges that faculty can face when starting genuinely interdisciplinary cyber programs. Although there is wide agreement that cyber security requires knowledge and skills across several disciplines, discipline-based incentives can prevent faculty from being able to pursue creative new program development. We hope the insights in this report help potential funders think about how to use their financial and social capital to support university leadership to overcome these barriers.

Given the varied interests of private foundations, we also want to highlight ideas that are not constrained by a commitment to fund university programs. These recommendations focus on how funders can address barriers to access that people of color can face entering the cyber field.

Key informants across our full sample see the opportunity that comes with taking a systemic perspective to identify where barriers to access originate and how they confront people who might otherwise enter the cyber field. Lack of access to economic resources, social networks, education and employment are all relevant. People identify these junctures as levers for philanthropic investment. We depict these ideas in Figure 11 below.

Among these opportunities, people prioritized investing in K-12 cyber education and supporting cyber programs at universities where student bodies are already predominantly diverse. We list specific programs and organizations we learned about in Appendix IV, knowing these are merely a few of many entrepreneurs and organizations committed to this topic. The framework in Figure 12 represents what we learned about the junctures (youth, education and training, and employment) and types of programs people see particularly relevant for philanthropic investment.

Figure 12: Opportunities to Address Barriers



VI CONCLUSION

The Hewlett Foundation's 2013 decision to establish a Cyber Initiative reflected a forward looking, timely shift to use philanthropic resources to address what is now one of the most pressing global security issues. From 2014-2020, the Cyber team granted $59 million to 23 US universities to create a talent pipeline the foundation believed would help increase the number of professionals equipped to advise policy makers on an increasingly complex domain. The foundation's approach was marked by two key tactics: giving a large sum of money to three relatively elite universities; and spreading the remaining funds across many different universities across the country. Hewlett's flexible giving approach – unrestricted monies and no prescriptive guidance on spending – allowed the university grantees to develop programs or projects that fit the constraints and opportunities of their respective contexts. Given the nascence of the field, the team sought to learn about different models of program maturity and quality and the influence that enablers might play in shaping program development and success.

The Hewlett Foundation commissioned this evaluation to take stock of its progress, develop a taxonomy of the portfolio's different cyber education models, share its learning with peer donors and inform the team's decisions about how best to spend the remaining resources during the last two years of the initiative. In

light of the 2020 racial justice movement and the foundation's commitment to diversity, equity and inclusion (DEI), the team elevated evaluation questions related to diversity and equity, seeking to understand for whom the Hewlett talent pipeline is working and why; which groups and communities are not being well-served; where the foundation team did and did not make progress in terms of integrating equity, inclusion and diversity into its approach and outcomes; and where it fell short.[41]

We found that all key informants agreed that interdisciplinary knowledge and skills are essential building blocks for cyber policy experts. An education pathway that privileges genuine multidisciplinary skill-building is a valid assumption to make about what is still needed in the sector. We learned that there is a difference between programs that offer cyber-focused courses across many disciplines, and those that define a new, intentional curriculum that requires students to take courses across disciplines. We learned that interdisciplinary program development can meet heavy resistance and identified enablers that include outside funding, senior level university sponsorship and inter-department collaboration and governance.

We also found that the more formal an interdisciplinary curriculum is, the more likely it is to last. We used our taxonomy to identify the 10 Hewlett grantees that have formalized, interdisciplinary programs and shared some of their promising practices in case studies. As with launching interdisciplinary programs, creating formal programs can have high transaction costs; many leaders with whom we spoke shared the challenges they faced turning an informal concentration, for example, into a degree program. By funding programs that combine these two elements, and encouraging university leadership to commit to them, the Cyber team can contribute to an education ecosystem that is capable of meeting the nation's need for qualified cyber practitioners.

The evolution of the Cyber Initiative suggests opportunities where the foundation team could have prioritized DEI goals sooner and consistent with the sector's 2018 analyses on the racial diversity gap. In retrospect, we see a blind-spot associated with the team's aspiration to solve for the lack of a certain capacity in a field by building a talent pipeline that goes from universities to employment without referring to the people that do and do not have access to this university pipeline in the first place. This mirrors what we learned across the university programs. Although diversity is increasingly defined as integral to cybersecurity and policy, its prioritization and integration with equity as part of cyber education is much less common. We found that six Hewlett grantee programs prioritize DEI with concrete practices. In our sample, more public universities prioritize diversity, equity and inclusion in their cyber programs, yet public schools received smaller grants and aggregate funding than private ones in the Hewlett portfolio.

The team has already begun to consider how to adjust its strategy in light of its 2020 commitment to DEI. This evaluation highlights promising practices that program leaders have used that the foundation can build upon to prioritize investments in a diverse, equitable and more inclusive cyber field. Many of our interviews and workshop conversations focused on the opportunities philanthropies have to include Minority-Serving Institutions in efforts like this one and assuring that they retain decision making power over any partnerships with other universities that result.

This is consistent with the two primary recommendations we heard from our key informants: that foundations support middle and high school opportunities for cyber education and mobility; and shift from an approach of encouraging predominantly white institutions to be more diverse, to one that supports program development at institutions where the student body is already diverse, and equity is a priority. Given Hewlett's traditional approach of partnering with universities, our recommendations center on the opportunities the Cyber team has to support public and minority-serving institutions to develop interdisciplinary, formal programs; replicate the NSF Scholarship for Service program; develop HBCU-led partnerships with leading cyber programs; and create an

[41] "Request for Proposals: Cyber Initiative Evaluation – Building a Talent Pipeline (University Grants)." *Hewlett Foundation*. 2020.

active learning effort to convene and advocate for other funders to support innovative cyber education models that prioritize DEI initiatives with concrete outcomes for students.

We conclude with our own learning about how impactful philanthropic concepts can be in signaling who is included and excluded from the benefit of foundation resources. The strongest feedback we heard was about the blind spot created by a strategy that neutralizes the structural barriers that many people face gaining access to economic, educational and employment opportunities. A recent piece about the "pipeline problem" in technology reflects this same point of view.

> "People have been talking about a pipeline problem in some form since the seventies…and that focus is always on individuals. It's on tracking people, not institutions and not structures. So this is why I think it continues to be a convenient excuse for a host of sins, because talking about a pipeline makes it seem as if all things are equal in the United States, and we just have to find a way to keep people in. But the truth is, when we think about a STEM pipeline, we don't talk about the fact that education in the United States is by no means equal from birth onwards."[42]

The two alternative frameworks we co-created with people demonstrate different ways philanthropies might consider building a field like cyber: one that identifies the potential barriers people face to access educational and employment opportunities; and another that presents recommended interventions for addressing these barriers. Our hope is that these frameworks and our efforts to channel the viewpoints we heard in our interviews and workshops help to deliver on equitable evaluation's promise to identify structural inequity and new opportunities for intervention.

[42] Megan Rose Dickey, "Examining the Pipeline Problem," *TechCrunch,* Feb 14, 2021.

Appendix I. Grant Descriptions

University Grantee	Total Funding	Purpose of Grant
American University	$750,000	To support the work of the think tank-style Internet Governance Lab
California Polytechnic State University	$502,000	To support the California Cybersecurity Institute's work to provide cybersecurity training to various actors
Carnegie Mellon University	$811,185	To support academic educational programs, as well as convenings between policymakers and academic cyber researchers
George Mason University	$625,000	To support research at their law school's National Security Institute, as well as applied training workshops for journalists, technologists, judges, and policymakers.
Georgetown University	$2,000,000	To fund the think tank-style Cyber AI project
Georgia Institute of Technology	$400,000	Supported research project on Mutual Legal Assistance treaties as pertains to cyber
Harvard University – Belfer Center	$1,500,000	To support the policy think tank-style Cyber Project
Harvard University – Berkman Klein Center	$1,863,000	To support the "Assembly" program, wherein students attend seminars, work on team-based projects, and complete a showcase.
Indiana University	$340,000	To fund the university's applied Cyber Clinic; its Cybersecurity Policy Bootcamps; and to launch the Midwest Cybersecurity Alliance to spread effective practices
Johns Hopkins University	$300,000	To support a new text; a workshop series; and a podcast on cybersecurity
Massachusetts Institute of Technology	$15,000,000	Anchor grantee – supported the creation of the Internet Policy Research Institute and a handful of classes
Middlebury College	$50,000	To fund a workshop (in partnership with New America) on cyber capacity building.
New York University	$1,385,379	To support an educational and research collaboration between the schools of law and engineering on the topic of cyber, including a master's program
Penn State University	$150,000	To create a free, internet-accessible textbook dealing with info security.
Stanford University	$15,049,876	Anchor grantee – supported the creation of the research-focused Cyber Policy Center, and a cyber concentration in an existing master's program.
Temple University	$150,000	To support a multi-day boot camp for professionals in the cyber sector who are not technical experts.
Tufts University	$453,000	To support the M.S. in Cybersecurity and Public Policy
University of California at Berkeley	$15,050,000	Anchor grantee – supported the creation of the Center for Long-Term Cybersecurity
University of Maryland	$59,670	To support a boot camp training program for journalists on cyber topics
University of Texas at Austin	$980,000	To support the cyber program at the university's Center for International Security and Law (including the creation of new pedagogical resources that are shared beyond the university).
University of Washington	$970,000	To support the policy think tank-like Tech Policy Lab
Virginia Tech	$700,000	To bring undergrads to DC for summer study on a variety of cyber and policy topics, and engagement with cyber policy professionals.
Yale University	$406,000	To support collaboration between the schools of law and computer science on a cyber education course

Appendix II. Key Informants

Name	Affiliation
Grantee Universities	
Laura DeNardis	American University
Martin Minnich	California Polytechnic State University
Kiron Skinner & Emily Half	Carnegie Mellon University
Jamil Jaffer & Jessica Jones	George Mason University
Ben Buchanan	Georgetown University
Peter Swire	Georgia Institute of Technology
Eric Rosenbach	Harvard University – Belfer Center
David O'Brien & Jonathan Zittrain	Harvard University – Berkman Klein Center
Scott Shakelford	Indiana University
Thomas Rid	Johns Hopkins University
Danny Weitzner & Taylor Reynolds	Massachusetts Institute of Technology
Elaine Korzak	Middlebury College
Randy Milch & Sarvenaz Bahktiar	New York University
Andrea Matwyshyn	Penn State University
Kelly Born & Andrew Grotto	Stanford University
Duncan Hollis	Temple University
Susan Landau	Tufts University
Ann Cleaveland & Lisa Ho	University of California at Berkeley
Robert Chesney	University of Texas at Austin
Ryan Calo & Joe Lott	University of Washington
Aaron Brantly	Virginia Tech
Oona Hathaway & Joan Feigenbaum	Yale University
Non-grantee Universities	
Antony Haynes	Albany Law School
Brian Gerber	Arizona State University
Kevin Powers	Boston College
Lethia Jackson	Bowie State University
Tony Coulson	California State University San Bernardino
Deidra Morrisson	Claflin University
Meritt Janow	Columbia University
Warren Eller	John Jay College
Jeff Kosseff	Naval Academy
Woodrow Hartzog	Northeastern
Geanie Umberger	Purdue University
Fatemeh Shafiei	Spelman College
Matthew Hudnall	University of Alabama
Maeve Dion	University of New Hampshire
Thomas Brunell	University of Texas at Dallas

Employers	
Bryan Ware	CISA
Dmitri Alperovitch	CrowdStrike
Nathaniel Gleicher	Facebook
Marian Merritt	National Initiative for Cybersecurity Education
Beth George	Wilson Sonsini
Professionals of Color in Cybersecurity[43]	
Keith Chapman	Belcan
Tendai Gomo	Google
Tony Marshall	Innovative Systems Group
Kemba Walden	Microsoft
Camille Stewart	Non-resident Cyber Fellow, Harvard Belfer Center; Google
Jeff Fields	Non-resident Joint Fellow, Harvard Belfer Center's Intelligence and Cyber Projects
Quiessence Phillips	NYC Cyber Command
Pinal Shah	Robinhood
Leo Pitt	SpectorOps
Kalika Dennis	Thompson Reuters
Martha Smith	Texas Facilities Commission
Nico Smith	
DEI Experts	
Larry Whiteside Jr.	International Consortium of Minority Cybersecurity Professionals
Aurelia T. Williams	CECOR (Consortium Enabling Cybersecurity Opportunities & Research); *also* Norfolk University
Theodore Hodapp	The Inclusive Graduate Education Network
Lynn Dohm	Women in Cybersecurity
Mary Chaney	Minorities in Cybersecurity
Travis York	ASPIRE: The National Alliance for Inclusive and Diverse STEM Faculty
Hewlett Staff	
Larry Kramer	Hewlett Foundation
Eli Sugarman	Hewlett Foundation
Monica Ruiz	Hewlett Foundation
Marlene Zapata	Hewlett Foundation

[43] All views expressed by key informants in this category are their own, and do not represent the views of their employers.

Appendix III. Case Studies

We include here case studies of both Hewlett grantee and non-grantee university programs that demonstrate promising practices to achieve high levels of interdisciplinarity; formality; or diversity, equity, and inclusion.

GRANTEE PROGRAMS

California Polytechnic State University

While hosted at a university, California Polytechnic State University, San Luis Obispo's (Cal Poly) California Cybersecurity Institute (CCI) is not an academic educational program. Instead, it focuses on implementing external workforce education and career boosting professional certifications that fall outside of the four-year university pipeline.

Working through industry partners, the CCI targets three distinct categories of people for training. The first category consists of blue-collar workers and targets building digital literacy for online safety and resiliency against phishing scams and other attacks. This training qualifies companies to bid on Department of Defense contracts, making it very attractive to industry partners - often opening doors to continued partnership to implement digital literacy and or additional trainings. The second category targets mid-level training at employees who are interested in learning more about cyber in order to upskill or to make a mid-career shift into a cyber-based role. This training is most often given to public sector and government employees. The final type of training is for higher-level leaders who want to gain advanced skills and knowledge about cybersecurity, particularly related to cloud computing.

The CCI also operates a statewide and nationwide K-12 program, concentrating on schools in disadvantaged areas catering to diverse students. The program exposes students to cyber topics like digital forensics and cryptography in fun, gamified environments like Virtual Reality. Students in turn get to build their cyber skills and are exposed to careers in the cybersecurity sector. This program began in 2016 with 40 students and will scale to 20,000 this school year. The programs are largely taught by CCI staff and Cal Poly student employees.

This year, the CCI plans to launch a pilot project with two California Community Colleges, members of Upskill California, and the California Employment Training Panel to help build out certification training programs with the goal of expanding to the remaining 27 Community Colleges.

Carnegie Mellon University

The cyber program at Carnegie Mellon University (CMU) conceives of diversity, equity, and inclusion as factors that are central to the success of the program. Led by Kiron Skinner, the program pursues this aim in several ways. First, it has instituted a training partnership with Spelman College - a Historically Black College or University – to support students there to develop the skills they need to become strong candidates for one of CMU's post-graduate cyber degrees.

Additionally, the program has brought on a staff member with a mandate to find ways to adjust their recruiting approach to enable the program to increase the proportion of diverse students who apply. As well, the program makes a point to bring in diverse campus speakers such as Condoleezza Rice to provide aspirational role models for their students. The program leaders also emphasize the importance of practicing an individualized mentorship across their diverse student body, so that students feel their voices are valued in the program.

CMU's cyber programs are housed within the university-wide Institute for Politics and Strategy, which is formally overseen by the deans of three different colleges – engineering, social sciences, and computing. The curricula offered in the cyber programs has been developed by all three schools.

George Mason University

George Mason University (GMU) offers interdisciplinary law and cyber programs that are designed to be accessible to broad array of communities.

The program grew out of an initial surveillance law class that Jamil Jaffer, the program director, began offering in 2009. He noticed that a large portion of the students were military veterans who were interested in the cyber security law domain but were pursuing degrees in intellectual property because it was the closest fit among available degrees at the time. With support from the dean of the law school, Jaffer began creating new classes that were better tailored to these students' interest, and then formalized the new offering into a Cyber Intelligence and National Security Law masters. These classes are also available to students as specialties in the school's JD and JM programs. All three programs focus on both law and policymaking.

Jaffer and his team take several other concrete – and innovative - measures to make the program accessible to more and different communities. First, they have designed a partnership with Hampton University, a Historically Black College or University (HBCU). By offering students their specialized ABA-certified training, they are able to admit those students to GMU's program without the need for LSAT scores. This allows the program to recruit diverse candidates who have received training in the skills and abilities they need to thrive in the program without the disincentive of diluting GMU's overall average LSAT score, which is a factor in school rankings. They are also building relationships with other HBCUs, women's colleges, and other Minority Serving Institutions to connect students at those schools with student mentors from GMU, who can provide guidance about navigating the sometimes-unclear career path in the cyber sector and can also share their own personal networks. Currently, in response to the national response to the death of George Floyd, Jaffer is working to design a partnership with Howard University – another HBCU. This partnership will experiment with ways to interest more people of color in the intelligence community, recognizing the barriers that exist due to the Black community's lack of full trust in the nation's policing and justice systems. He and his team are also working to increase the proportion of female professors, and to be more intentional about recruiting Black fellows. Finally, many of the program's classes are taught at night. While this is a function of the scheduling needs of some of the real-world practitioners who teach the classes, it also allows students from a wider mix of backgrounds and career stages to pursue degrees.

Indiana University

Indiana University's interdisciplinary cybersecurity program places a premium on applied learning, offering its students ample opportunities to gain real-world experience in addressing cyber threats.

The Cybersecurity Program at Indiana University (IU) is the result of a formalized alliance between three of the University's top colleges—the Kelley School of Business, the Maurer School of Law, and the Luddy School of Informatics, Computing, and Engineering. Growing from an initial Provost directive in 2014 to establish more graduate-level cybersecurity certificates, the Program now offers an M.S. in Cybersecurity Risk Management, a Ph.D. minor in Cybersecurity Risk Management, and dual degree options including a JD-M.S. in Cybersecurity Risk Management that can be completed in three years and an MPA-M.S. in Cybersecurity Risk Management.

In addition to more typical cyber policy classes, Indiana's program also offers several hands-on learning experiences. These include service-learning opportunities such as the IU Cybersecurity Clinic. Through this applied course, students work with local critical infrastructure providers—such as local governments, small utilities, and nonprofit organizations — on real-world projects to improve their cybersecurity resilience. The Clinic typically works with clients that do not have the resources to acquire these services elsewhere. Aside from the IU Cybersecurity Clinic, the Program also offers a travel-embedded capstone course through

which students work with civil society groups such as Consumer Reports and international clients like NATO CCDCOE. The Program is also a Hacking for Defense (H4D) partner and a member university in the NSF's CyberCorps SFS Program, providing further opportunities for students to apply what they have learned for DoD clients and civilian government clients.

The Program also administers a paid cybersecurity internship program, connecting students with partner organizations to provide additional exposure to the practical application of cybersecurity best practices. These Cyber Peace Internships are supported through a combination of university funding and external grants, giving students of all means an opportunity to participate.

This combination of interdisciplinary coursework and applied service-learning opportunities aims to provide Program graduates with the relevant knowledge, practical skills, and hands-on experience to give them confidence as they enter the cybersecurity workforce.

UC Berkeley

UC Berkeley's online interdisciplinary Master of Information and Cybersecurity (MICS) program provides an example of how an anchor grantee prepares students for leadership roles in cyber, with a particular emphasis on the importance of supplementing theoretical learning with hands-on experience.

This orientation towards combining analytical and practical learning can be seen in their Citizen's Clinic program. Modelled on law and medical clinics, this experiential program brings together several dozen Berkeley students each year with under-resourced non-profits who need cybersecurity support in semester-long and multi-semester collaborations. The students who participate are drawn from all campus disciplines, including law, cybersecurity, social sciences, engineering, and more; for some, it is their first exposure to the cyber field. The course is taught by faculty from Berkeley's Center for Long-Term Cybersecurity and School of Information.

The more traditional classes in the master's in cybersecurity program also place a premium on marrying the academic with the applied. In the Privacy Engineering advanced elective, students build models and implement algorithms to protect against confidentiality, anonymity and inference risks. Additionally, security tool labs, incident response scenarios, and the capstone team projects which build on an "ideation-plan-build-pitch" process further strengthen students' real-world experience. The professors comprise both Berkeley campus faculty as well as industry experts and practitioners, to provide the program's students with both the conceptual understanding and the practical skills needed to effectively direct and implement cybersecurity strategy and operations.

The program also invests in student outcomes by providing a career advisor dedicated to its cybersecurity students, in addition to the more generalized career services available from the larger university. This support was put in place once their first cohort of students began graduating, to help students navigate the cybersecurity sector's complex ecosystem of subdomains and unique job search challenges.

University of Texas at Austin

The cyber program at UT Austin is distinctive in its orientation towards creating interdisciplinary resources that can be used both within the program and by the public.

Five years ago there were no cyber policy or law classes available at UT Austin - just the highly-technical courses offered by the Computer Science department. Bobby Chesney, Director of the campus-wide Robert Strauss Center for International Security and Law, set out to change this. He created a foundational survey course designed to introduce students from any disciplinary background to the cyber security sector. The goal of the course was to help students understand cyber's relevant institutions, its legal frameworks, its core policy disputes, and its business interests in order to help people from different disciplinary backgrounds understand one another.

That first class was structured around a casebook Chesney created, which was recently made public by the Strauss Center. The book has been downloaded over 5k times since its launch in March 2020, and it is a required text in at least one other university program. Soon after the Center launched this class it created a companion course that provides a grounding in basic cyber technology for non-technical students, taught by technologists who are skilled at translating the material for laypeople. The Strauss Center intends to publicly share these curricular resources as well, once they are perfected.

The Center's next priority is to launch a comprehensive cyber job information portal that can be used by both its own students and the public.

Virginia Polytechnic Institute and State University (Virginia Tech)

The cyber program at Virginia Tech offers an interdisciplinary educational experience designed with equity in mind.

The school has recently completed the first semester of its new Integrated Security minor, a cross-college program that unites what it calls cyber and "human" education. The program's faculty advisor, Aaron Brantly, institutionalizes the classes Virginia Tech has been offering to undergraduates for the past several years by formalizing a course of study that spans the colleges of engineering, business, and liberal arts into one cohesive course of study. This includes traditional classes as well as applied exercises like cyber crisis simulations.

Due to its location in norther Virginia, roughly half of the students in the program are people of color. The program specifically engages with questions of equity in its curriculum – for example, classes will consider issues like the varying access to digital infrastructure different communities enjoy. All of the program's courses were evaluated last year to ensure they engaged with such questions before the minor was formally established. Additionally, the students are given access to a Tech4Humanity lab and the Integrated Security Research Education Center where they are encouraged to explore ideas they are passionate about, so that they have a space in which to think beyond issues that often receive precedence in cyber research, including issues that are particularly relevant to their own communities. Students are encouraged to examine complex challenges at the intersection of cybersecurity and human, economic, and environmental security.

NON-GRANTEE UNIVERSITY CYBER PROGRAMS

Arizona State University

Arizona State University's program integrates cyber with emergency management, a highly synergistic disciplinary union that is less commonly seen than other pairings such as law, business, or international relations.

Brian Gerber, the academic director of the Master of Arts in Emergency Management and Homeland Security program, describes emergency management as an inherently interdisciplinary profession as its core purpose is to provide a coordinating function across different actors and operational areas in managing responses to emergencies and disaster. Recognizing the growing threat of cyber-caused kinetic emergencies (such as cyber attacks aimed at disrupting critical infrastructure assets such as transportation systems, utilities, dams, etc.), this program aims to give its students the grounding in cybersecurity policy they will need in order to coordinate responses to such challenges. It combines introductory technical cyber courses with additional coursework on the US cybersecurity policy ecosystem, with the goal of producing emergency management practitioners who have the cyber fluency to work with technical challenges and interact with technical professionals.

Inclusion of a cyber focus area within the program promotes interdisciplinary learning by design, as disaster by definition crosses domains and disciplines. It is hosted in the Watts College of Public Service and Community Solutions, which consists of four schools. The program utilizes courses from all four of these schools, as well as from the University of New South Wales in Australia. The faculty are a mix of academics and active emergency management and homeland security practitioners. The cybersecurity focus area is structured as a formal concentration within the larger MA EMHS degree.

This program is fully online, which makes it accessible to its students who are mainly early and mid-career practitioners and those transitioning from military service to civilian careers. Flexibility is especially important to such a student population, as deployments to disaster incidents or for military obligations are common during any given semester.

The MA EMHS program strives to promote and maximize diversity in its student population in order to address the issue of underrepresentation in the emergency management profession. The program has conducted outreach to HBCUs (for example, Jackson State University); engaged with the Bill Anderson Fund fellows program which promotes greater minority representation in educational and professional fields related to hazards and disasters; and has successfully cultivated a diverse student population, consistent with ASU's approach in this area.

California State University at San Bernardino

The California State University at San Bernardino (CSUSB) is a national leader in cyber university programs. Under the direction of Tony Coulson, CSUSB manages the CAE (Center of Academic Excellence) Community, which is the body that works to support and align the efforts of the 335 colleges and universities that the NSA has designated as centers of academic excellence in cybersecurity. These include defense academies, research universities, and educational institutions that offer both technical and interdisciplinary cyber programs. In partnership with government and industry, the CAE Community provides supportive resources to these schools and enables cross-institutional learning by facilitating symposia and other community learning events addressing faculty and student development, workforce initiatives, and K-12 pipelines. Currently, CSUSB is partnering with the NSF and Whatcom Community College as the co-lead on a pilot program called the Collaborative Community College Pilot that will provide new funding to cyber programs at community colleges, modelled on the CyberCorps: Scholarships for Service program. They are also funding a study to assess the feasibility of a national K12 CAE program, which would create an integrated curriculum and designate qualified schools to create a clear pathway into further cyber education for young students.

In addition to this work as a national leader in the university cyber sector, CSUSB's own program offers three master's degrees (as MS in Information Systems and Technology, an interdisciplinary master's in National Cyber Security Studies, and an MBA and MPA). CSUSB also offers three bachelor's programs and as well as a cyber certificate. Utilizing a modular approach, these programs span business, IT, criminal justice, security studies, and policy. The curricula for these programs were made to solve for workforce competency gaps that CSUSB identified in conversation with industry and government employers when they began their program ten years ago.

Norfolk State University

Norfolk State University is one of the leading Historically Black College or Universities (HBCUs) in the cyber sector. Currently directed by Dr. Aurelia Williams, the program began in 2003 with a computer science masters that offered a cyber security emphasis. It then grew to offer an online cyber security masters that welcomes both technical and non-technical students. Just this past fall, the program launched its newest offering - the nation's first master's degree in cyber psychology, training students to address deviant behavior such as hacking online.

Due to the strength of it programs, Norfolk was elected by twelve of its peer HBCUs to lead a government-sponsored consortium of these universities alongside two national labs. The Consortium Enabling Cybersecurity Opportunities and Research (CECOR)'s goal is to improve the flow of HBCU graduates into cyber roles in the government. As some of the participating universities cyber programs are more interdisciplinary and formalized than others, one of the functions of the consortium is to share learnings and mentorship between universities to support the members to develop the strength of their programs. Additionally, several of the HBCUs in the group conduct K12 cyber programs at local schools to set more young people of color on a path to enter university cyber programs. As leader of the group, Norfolk oversees this body of work.

Within its own cyber program, Norfolk places a premium on student outcomes. They offer students summer research positions and access to relevant boot camps to help ensure that they are job-ready upon graduation. They also emphasize the importance of internship experiences. Recognizing that one of the challenges of the cyber career path is a lack of common knowledge of what the opportunities are, Norfolk partners with relevant employers to ensure that they have a presence on campus so that students are aware of them from their freshman year. The result is that the students have time to investigate the internship opportunity and plan to incorporate it into their time at the university.

Appendix IV: Cyber Programs and Initiatives

We learned about programs and initiatives that work to address different aspects of the workforce gap – particularly the need for improved diversity, the need for early exposure to cyber, and the need for applied educational experiences. We provide examples that people identified during our interviews and conversations.

K12 PROGRAMS

Below are initiatives which work to expose K12 students to cyber, through either direct education or the provision of curricular resources. These initiatives are operated by non-profits, private industry, and the government.

Name	Description	Program Link
GenCyber	NSA/NSF-led K12 cyber summer camps, often offered in partnership with schools and universities	https://www.gen-cyber.com/about/
Cyber Patriot	Air Force Association-led initiative offering cyber camps and competitions to K12 students	https://www.uscyberpatriot.org/
Girls Go CyberStart	Self-directed educational resources + cyber competition for girls. It is operated by SANS and sponsored by National Governors Association	https://www.cyberstartus.org/
Girl Scout Cyber Security Badges	Introduction to cyber training for girl scouts.	https://www.girlscoutshop.com/Junior-Cybersecurity-Badge-Requirement-Pamphlet
Belcan Academy	Provide training resources and certifications for high school students and current professionals to enter cyber	https://www.belcancyberacademy.com/hs
Cyber.org	Free resources for teachers who want to incorporate cyber instruction in their classes	https://cyber.org/
National Cyber Group	A K-12 cyber education initiative offered in partnership with Discovery Education	https://www.natcybergroup.com/ncep
National Cyber League	Platform that simulates cyber threats + a competition for high school and college students to respond to cyber threats.	https://nationalcyberleague.org/
Hacker Highschool	A complete, self-guided curriculum for cyber safety and cybersecurity designed for teens from 12-20 years old.	https://www.hackerhighschool.org/
idTech	Cyber camps for teens offered by a private company (for a fee)	https://www.idtech.com/courses/cybersecurity-and-encryption
U.S. Cyber Academy	Week-long camp, operated by Space Camp. Offered for a fee.	https://www.spacecamp.com/cyber/academy
TechGirlz Cybersecurity Camp	Free resources and guidance for educators interested in staging cyber camps for girls	https://www.techgirlz.org/camp/cybersecurity/

U.S. Cyber Challenge	Week-long training camp for teams that also includes a job fair and a "capture the flag" exercise.	https://www.uscyberchallenge.org/cyber-camps
PowerUp: Cyber Games	Middle and high school instruction paired with ongoing cyber competition, targeted at students in the Midwest.	https://wecyberup.org/inspire-youth/
CAE K12 Pipeline Program: Regions Investing in the Next Generation (RING)	Provides an online cybersecurity fundamentals course targeting rural, under resourced school systems; home school students; and schools without an established cybersecurity program	https://www.caecommunity.org/sites/default/files/NCAE-C%20Initiatives%20Guide%202021.pdf

Apprenticeship Programs

These initiatives are government-accredited programs that combine classroom learning with on-the-job training. Some are spearheaded by colleges, some by private companies, and some by non-profits.

Name	Description	Link
Purdue Cyber Apprenticeship Program	Apprenticeship program offered by Purdue University in partnership with local industry. All students attain an associate's degree, at minimum.	https://centers.purdue.edu/pcap/
ISG Cybersecurity Apprenticeship Program (ISG-CAP)	Apprenticeship program offered by the for-profit company Innovative Systems Group	https://isglink.com/
CICESS Peoria	Apprenticeship program offered through partnership of 9 Illinois community colleges and local industry.	https://www.peoriamagazines.com/ibi/2015/apr/jobs-and-cybersecurity
CICESS San Antonio	Apprenticeship program offered through partnership of Alamo Community College, Project Quest, and local industry	https://ishpi.net/cicess-san-antonio/
Harper College Cyber Security Apprenticeship Program	Apprenticeship program offered through partnership between Harper College and local industry	https://www.harpercollege.edu/apprenticeship/cybersecurity/index.php
Tideater College Cyber Apprenticeship Program	Apprenticeship program offered through partnership between Tidewater Community College and Peregrine Technical Solutions LLC	https://augustafreepress.com/mcauliffe-announces-virginias-first-cybersecurity-apprenticeship-program/
University of Maryland, Baltimore College	Apprenticeship program offered through partnership between University of Maryland, Baltimore College and local industry	https://www.umbctraining.com/training-centers/about-us/apprenticeship

Midwest Cyber Center Cyber Apprenticeship	Apprenticeship program operated by nonprofit Midwest Cyber Center in partnership with local industry	https://www.stlouis-mo.gov/government/departments/slate/slate-mo-career-center/cyber-security-analyst.cfm
CyberUp	CyberUp's LevelUp program trains and places candidates with industry partners in the midwestern region	https://wecyberup.org/educate/

Other Training Initiatives

Below are training programs and resources, other than apprenticeships and K12 programs.

Name	**Description**	**Link**
Federal Virtual Training Environment (FedVTE)	Program of the National Initiative for Cybersecurity Careers and Studies (a subset of CISA) to provide free online online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, US military veterans and the public.	https://niccs.us-cert.gov/training/federal-virtual-training-environment-fedvte
NICCS Training Catalogue	Government catalog of cybersecurity training courses across the US. 5k+ courses.	https://niccs.us-cert.gov/
Diversity Cyber Academy	Free training course in cyber for people of color	https://www.sans.org/cybertalent/cybersecurity-career/diversity-cyber-academy
Cisco Global Cybersecurity Scholarships	Scholarship for cybersecurity certificate training	https://mkto.cisco.com/Security-Scholarship.html
Cybersecurity Talent Initiative	Microsoft, Mastercard, Workday/ federal government partnership to train and employ cybersecurity students in the public and then private sector	https://www.healthcareitnews.com/news/microsoft-mastercard-workday-help-create-cybersecurity-talent-initiative
NICE Challenge	Develops real-world cybersecurity challenges within virtualized business environments that "bring university students the workforce experience before the workforce."	https://nice-challenge.com/
NSA College of Cyber	NSA's internal cybersecurity training program for staff. They also work with universities to align their curriculum to what the NSA needs to hire for.	https://www.military.com/education/2014/08/29/the-nsas-school-of-cyber.html

Diversifying University Education

Below are initiatives working to improve diversity in university-based education programs, both by supporting new Minority Serving Institution entrants and by improving diversity at Primarily White Institutions.

Name	Description	Link
CECOR (Consortium Enabling Cybersecurity Opportunities & Research)	Partnership btw national labs and HBCUs to funnel more BIPOC into cybersecurity jobs with federal government. Has K12 programs too.	http://cecork-12.com/
Cybersecurity Education Diversity Initiative	Collaboration with CAE program and DoD to support Minority Serving Institutions interested in establishing cyber programs.	https://www.nsa.gov/news-features/press-room/Article/2382623/department-of-defense-and-national-security-agency-announce-new-cybersecurity-i/
The Inclusive Graduate Education Network	A bridge program that supports STEM students of color without the credentials to be accepted at PhD programs transition into them. While cyber is not one of their disciplines, they have expressed an interest in developing a program for it.	https://www.igenetwork.org/
Cybersecurity Education Diversity Initiative (CEDI)	A DoD- and NSA-sponsored program that helps MSIs improve their cyber offerings by pairing them with existing cyber CAEs for mentorship	https://www.nsa.gov/news-features/press-room/Article/2382623/department-of-defense-and-national-security-agency-announce-new-cybersecurity-i/

Affinity Groups

Below are groups and associations that support BIPOC or women in cyber careers by offering mentorship, networking, and professional development opportunities.

Name	Description	Link
International Consortium of Minority Cybersecurity Professionals	Industry association working toward improved professional advancement of BIPOC in cyber.	https://www.icmcp.org/about-us
The Diana Initiative	A conference for women in information security	https://www.dianainitiative.org/
Women in CyberSecurity (WiCyS)	A community of engagement, encouragement and support for women in cybersecurity.	https://www.wicys.org/
Minorities in Cybersecurity	A community of BIPOC cybersecurity professionals that supports its members to excel in the cybersecurity field.	https://www.mincybsec.org/

Blacks in Cybersecurity	A conference series, meetup group, and social organization working to address the disparity between the Black community and Cybersecurity knowledge and resources.	https://www.blacksincyberconf.com/faqs
Women's Society of Cyber Jutsu	Works to advance women in cybersecurity careers by providing programs and partnerships that promote hands-on training, networking, education, mentoring, and resource-sharing.	https://womenscyberjutsu.org/page/WhoAreWe
LATAM Women in Cybersecurity	Advance the careers of Latinas in cyber through education and mentoring initiatives	https://www.womcy.org/
Black Girls Hack	Shares knowledge and resources to help black girls and women breakthrough barriers to careers in information security and cyber security.	https://blackgirlshack.org/
Black Cybersecurity Association	Trainings and networking for Black people in cybersecurity	https://blackcybersecurityassociation.org/
NPower	Creates pathways to digital careers for military veterans and young adults from underserved communities (not confined to cyber)	https://www.npower.org/about/
Black in Computing	Addresses systemic racism in the technology sector (not confined to cyber).	https://blackincomputing.org/
Black ComputeHER	Shares access to opportunities and training for Black women in the technology sector (not confined to cyber).	https://blackcomputeher.org/about-us/
Women of Color Advancing Peace and Security: Cyber Security and Emerging Technologies Working Group	Works to advance the leadership and professional development of women of color in the field	https://www.wcaps.org/workinggroup/cybersecurity
#SharetheMic	Began as a social media campaign to amplify women and POC in cyber; now offers network that shares professional and training opportunities	https://sharethemicincyber.splashthat.com/

Other Relevant Cyber Initiatives

Name	**Description**	**Link**
(ISC)2	International, nonprofit membership association for information security leaders	https://www.isc2.org/about
NCYTE Center	Invests in technological innovation, resources, professional development and tools to support community colleges.	https://www.ncyte.net/about-us/about
Cyberseek	Cybersecurity career pathway visualization tool; sponsored by the federal government	https://www.cyberseek.org/pathway.html
CAE Community	Supports and aligns the efforts of the 335 universities the NSA has designated centers of academic excellence in cybersecurity	http://caecommunity.org/
JourneysMap	interactive pilot to map cyber education, trainings, certifications and career pathways.	https://sdccoe.org/careermap/

Appendix V: Evaluating the Talent Pipeline Measurement System

The Hewlett Foundation Cyber Initiative defined implementation markers or measures to signal progress of its portfolio. To gather data, the team conducted an annual survey of grantees. In this section, we describe the methodological challenges that made it difficult to use this system as a reliable source of information for the evaluation. Our hope is that these insights can support the team's revised approach.

TABLE 3: PROGRESS OF IMPLEMENTATION MARKERS

Marker	Latest Year Performance
Curriculum maturity – grantees are making substantial progress toward establishing an interdisciplinary cyber program including courses, modules or degrees	☐ Across the portfolio, at least 6 different disciplines are offered. ☐ From 2016 to 2019, the number of program types offered increased from 2 to 5.
Diverse & Accomplished staff – grantees' faculty, staff, fellows are increasingly interdisciplinary and new / open positions are being filled quickly.	☐ In 2019, Hewlett grantees' faculty have a diversity of disciplinary backgrounds; only 29% have computer science background.
Student outcomes – majority of graduating students are entering the of cyber policy and heading to positions in a diversity of industry types.	☐ Insufficient data on student placement
Diversified funding – grantees are on a path to financial sustainability evidenced by Hewlett making up a smaller yearly % of budget and hiring of non-policy staff.	☐ On average in 2019, Hewlett makes up 27% of grantees' total funding ☐ On average in 2019, 88% of grantees' total funding comes from their three largest funders

The table above provides the Talent Pipeline markers and the data generated through the foundation's measurement approach. In short, we find these data difficult to interpret due to three major challenges:

We identify 3 major challenges with the way the measures are defined, and the data are collected.

1. The measures are imprecise and therefore do not reflect meaningful outcomes. The two examples of this challenge are how the foundation defines interdisciplinarity and diversity, equity and inclusion. The former is measured in terms of the types of classes offered at a particular university rather than whether students actually take classes across disciplines. To measure grantee efforts in DEI, the foundation system asks grantees an open qualitative question without a specific definition or framework to capture meaningful information about how programs prioritize or make changes over time.

2. The target student population is not consistently defined and so survey respondents report information on students that are not directly engaged in their cyber education programs. This creates an issue because Hewlett's system tracks progress of activities that the foundation does not support. Another example is the concept of a "program." Because this word is not defined for grantees to understand how the foundation defines the term when they complete the foundation survey, several grantees report on research rather than education programs that do not have implications for creating new policy experts.

3. The sample of university programs changes over time, presenting challenges to the foundation's ability to make any meaningful conclusions about trends or progress. There are two sampling issues with the current survey approach. The first is that the universe of programs changed as new grants were made during the 2015-2020 period. It is more appropriate, therefore, to say that the foundation's survey data represent snapshots in time rather than making conclusions that there are changes over time experienced by the same set of grantees. The second sampling issue is that the unit of analysis is sometimes the individual rather than the university program. We find this to be especially problematic when the team seeks to measure the make-up of faculty. For example, when measuring the disciplinary composition of faculty, data reflect all individuals as if they were

at one institution rather than the composition of an individual program and diversity of faculty within it. One can't conclude, therefore, if grantee program faculty are becoming more or less diverse over time.

Our recommendation is that the Cyber team decide on its priorities for the next two years before revising the implementation markers and/or the annual survey. This will help the team to figure out what is most important to achieve, the metrics that will signal that change the most accurately, and the data that can help the team learn what happens across the grantee population over this next period of time.

Appendix VII: References

Aspen Cybersecurity Group, "Principles for Growing and Sustaining the Nation's Cybersecurity Workforce", *The Aspen Institute,* November 8, 2018. https://www.aspeninstitute.org/publications/principles-for-growing-and-sustaining-the-nations-cybersecurity-workforce/.

Blair, Jean R.S., Andrew O. Hall and Edward Soblesk. "Educating Future Multidisciplinary Cybersecurity Teams." *Computer*, Volume: 52, Issue: 3, March 2019.

Bolton, T., Inglis, C., "Improving Cyber-Oriented Education, One Cyber Clinic at a Time", *Lawfare,* August 13, 2020. https://www.lawfareblog.com/improving-cyber-oriented-education-one-cyber-clinic-time.

Boulton Reporter, Clint. "Snowden Effect Dominates 2013 Tech Industry News." *Wall Street Journal*, December 26, 2013. https://blogs.wsj.com/cio/2013/12/26/snowden-effect-dominates-2013-tech-industry-news/.

Bracey, Earnest N. "The Significance of Historically Black Colleges and Universities (HBCUs) in the 21st Century: Will Such Institutions of Higher Learning Survive?" *American Journal of Economics and Sociology* 76, no. 3 (2017): 670–96.

Bumiller, Elizabeth and Thom Shanker, "Panetta Warns of Dire Threat of Cyberattack on U.S." *The New York Times,* October 11, 2012. https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.htm

Burrell, D. N. "Developing More Women in Managerial Roles in Information Technology and Cybersecurity." 2019. /paper/Developing-more-Women-in-Managerial-Roles-in-and-Burrell/6f0e736b1373aaf842f73b9f9fcfb8341649ca36.

Caldwell, Tracey. "Plugging the Cyber-Security Skills Gap." *Computer Fraud & Security* 2013, no. 7, 5 – 10, July 1, 2013. https://doi.org/10.1016/S1361-3723(13)70062-9.

Carlin, J., "Major Employers Commit to Build a Stronger Cybersecurity Workforce Pipeline," *The Aspen Institute,* October 30, 2019. https://www.aspeninstitute.org/programs/cybersecurity-technology-program/aspencyber-workforce-pipeline/.

Chairman of the Joint Chiefs of Staff, "The National Military Strategy of the United States of America," Washington, DC: Joint Chiefs of Staff, 2004. www.defense.gov/news/mar2005/d20050318nms.pdf.

Coffman, Julia, "Equitable Evaluation is for All", *Equitable Evaluation Initiative,* October 2019. https://www.equitableeval.org/blog-main/2019/10/16/equitable-evaluation-is-for-all-evaluation

"Command History." *U.S. Cyber Command*. https://www.cybercom.mil/About/History/.

Commerce, U. S. Department of, and U. S. Department of Homeland Security. "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future", *52 – 52*, May 30, 2018.

Coulson, Tony, Megan Mason, and Vincent Nestler. "Cyber Capability Planning and the Need for an Expanded Cybersecurity Workforce." *Communications of the IIMA* 16, no. 2, February 4, 2019. https://scholarworks.lib.csusb.edu/ciima/vol16/iss2/2.

"Cyber Initiative Grantmaking Strategy", *Hewlett Foundation,* 2017. https://hewlett.org/library/cyber-initiative-grantmaking-strategy/

"Cybersecurity Supply And Demand Heat Map." *Cyberseek*. https://www.cyberseek.org/heatmap.html.

"The Cybersecurity Workforce Gap." https://www.csis.org/analysis/cybersecurity-workforce-gap.

"Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", *United States Executive Office of the President,* April 3, 2014. https://fas.org/irp/eprint/cyber-review.pdf

"Cybersummit 2020 Day Three: Diversity In Cybersecurity", *Cybersecurity and Infrastructure Security Agency,* 2020. https://www.cisa.gov/cybersummit-2020-day-three-diversity-cybersecurity.

Diakun-Thibault, Nadia. "Defining Cybersecurity." *Technology Innovation Management Review,* 2014.

Dickey, M. R., "Examining the Pipeline Problem," *TechCrunch,* Feb 14, 2021. https://techcrunch-com.cdn.ampproject.org/c/s/techcrunch.com/2021/02/14/examining-the-pipeline-problem/amp/

Equitable Evaluation. "Equitable Evaluation Framework™." https://www.equitableeval.org/framework.

"Evaluation of Network Building: Grants and Beyond-Grant Activities", *Camber Collective,* 2016. https://www.hewlett.org/wp-content/uploads/2018/02/Evaluation-of-network-building-Cyber-2018.pdf.

Evans and Reeder, "A Human Capital Crisis in Cybersecurity", *Center for Strategic and International Studies,* November, 2010. https://www.csis.org/analysis/human-capital-crisis-cybersecurity.

Evans and Reeder, "A Human Capital Crisis in Cybersecurity", *Center for Strategic and International Studies,* 2016.

Reed, J., Aosta-Rubio, J., "Innovation Through Inclusion: The Multicultural Cybersecurity Workforce," *Frost & Sullivan*. https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

Graff, G., "DOJ Indicts 9 Iranians for Cyber Heists Against 144 Colleges." *Wired*. March 23, 2018. https://www.wired.com/story/iran-cyberattacks-us-universities-indictment/.

Grobe, Terry. "Better Careers for Californians: Innovations That Build the Talent Pipeline. *Jobs for the Future*, 2019. https://eric.ed.gov/?id=ED603622.

"H.R. 258 – 48." *U.S. House of Representatives*. https://csrc.nist.gov/CSRC/media/Projects/Risk-Management/documents/FISMA-final.pdf.

Hadley, James. "To Help Tackle Workforce Shortage, Cybersecurity Needs To Address Unconscious Bias In Hiring", *Forbes,* August 6, 2020. https://www.forbes.com/sites/jameshadley/2020/08/06/to-help-tackle-workforce-shortage-cybersecurity-needs-to-address-unconscious-bias-in-hiring/.

Holmes, Oscar, Kaifeng Jiang, Derek R. Avery, Patrick F. McKay, In-Sue Oh, and C. Justice Tillman. "A Meta-Analysis Integrating 25 Years of Diversity Climate Research." *Journal of Management*, June 29, 2020, 0149206320934547. https://doi.org/10.1177/0149206320934547.

Hurd, Will. "H.R.2454: Department of Homeland Security Data Framework Act of 2018", *U.S. House of Representatives,* 2017/2018. https://www.congress.gov/bill/115th-congress/house-bill/2454.

J. Dean-Coffey, J. Casey, & L. D. Caldwell, "Raising the Bar — Integrating Cultural Competence and Equity: Equitable Evaluation." *The Foundation Review,* 6(2), 81–94, 2014.

Kramer, L., "Committing to Diversity, Equity and Inclusion," *Hewlett Foundation,* January 2018. https://hewlett.org/committing-diversity-equity-inclusion/

"Internet Governance - The Snowden Effect" *The Economist*, January 24, 2014. https://www.economist.com/babbage/2014/01/24/the-snowden-effect.

"(ISC)² Cybersecurity Workforce Study, 2020: Cybersecurity Professionals Stand Up to a Pandemic", *(ISC)², 2020.* "(ISC)²ResearchDrivenWhitepaperFINAL.Pdf." https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx?la=en&hash=2879EE167ACBA7100C330429C7EBC623BAF4E07B.

"Women in Cybersecurity: Young, Educated, and Ready to Take Charge: An (ISC)² Cybersecurity Workforce Report", *(ISC)², 2018.* https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx?la=en&hash=4C3B33AABFBEAFDDA211856CB274EBDDF9DBEB38.

"(ISC)² 2020 Cybersecurity Workforce Study", *(ISC)², 2020.* https://www.isc2.org:443/Research/Workforce-Study.

Kay, David J., Terry J. Pudas, and Brett Young. "Preparing the Pipeline: The U.S. Cyber Workforce for the Future:" Fort Belvoir, VA: Defense Technical Information Center, August 1, 2012. https://doi.org/10.21236/ADA577318.

Larsen, S., "Every Single Yahoo Account Was Hacked - 3 Billion in All", *CNN Business,* October 4, 2017. https://money.cnn.com/2017/10/03/technology/business/yahoo-breach-3-billion-accounts/index.html.

Makridis, Christos. "Expand The Talent Pipeline: Focus On Skills, Not Degrees." *Forbes,* June 29, 2020. https://www.forbes.com/sites/christosmakridis/2020/06/29/expand-the-talent-pipeline-focus-on-skills-not-degrees/.

Marks, J., "The Cybersecurity 202: DHS Is Highlighting Diversity as a Key Cybersecurity Goal", *The Washington Post*, September 29, 2020

Maughan, D., William Newhouse, and T. Vagoun. "Introducing the Federal Cybersecurity R&D Strategic Plan" 19, no. 4, 3–7, December 14, 2012.

Mazetti, Mark and David Sanger, "Security Leader Says US Would Retaliate against Cyberattacks." *The New York Times,* March 12, 2013. https://www.nytimes.com/2013/03/13/us/intelligence-official-warns-congress-that-cyberattacks-pose-threat-to-us.html

Miller, Claire Cain. "Revelations of N.S.A. Spying Cost U.S. Tech Companies." *The New York Times*, March 21, 2014, sec. Technology. https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

Miller, J., Gosler, J., "Final Report of the Defense Science Board (DSB) Task Force on Cyber Deterrence", *Defense Science Board, U.S. Department of Defense,* February, 2017. https://www.armed-services.senate.gov/imo/media/doc/DSB%20CD%20Report%202017-02-27-17_v18_Final-Cleared%20Security%20Review.pdf.

Steve Morgan, "2021 Directory of M.S. In Cybersecurity Programs At Universities In The U.S.", *Cybercrime Magazine,* January 11, 2021. https://cybersecurityventures.com/cybersecurity-university-masters-degree-programs/

Mutune, George. "The Quick and Dirty History of Cybersecurity." CyberExperts.com, July 21, 2019. https://cyberexperts.com/history-of-cybersecurity/.

"National Protection and Programs Directorate (NPPD) at a Glance", *Cybersecurity & Infrastructure Security Agency*. https://www.cisa.gov/publication/nppd-glance.

"NICE Framework Resource Center." *NIST*. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center.

Paletta, Damian. "U.S. Blames Russia for Recent Hacks." *Wall Street Journal*, October 7, 2016, sec. Politics. https://www.wsj.com/articles/u-s-blames-russia-for-recent-hacks-1475870371.

Perhach, Paulette. "The Mad Dash to Find a Cybersecurity Force." *The New York Times*, November 7, 2018, sec. Business. https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html.

Peterson, Andrea. "The Sony Pictures Hack, Explained." *Washington Post*. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

"Request for Proposals: Cyber Initiative Evaluation – Building a Talent Pipeline (University Grants)." *Hewlett Foundation.* 2020.

Sanger, D., Corasaniti, N., "D.N.C. Says Russian Hackers Penetrated Its Files, Including Dossier on Donald Trump", *The New York Times,* June 14, 2016. https://www.nytimes.com/2016/06/15/us/politics/russian-hackers-dnc-trump.html.

Senator Angus King, Representative Mike Gallagher, "Cyberspace Solarium Commission White Paper #3: Growing a Stronger Federal Cyber Workforce", *Cyberspace Solarium Commission.* https://www.solarium.gov/public-communications/workforce-white-paper.

Sian, J., "Why We Need More Diversity in Cybersecurity," *Microsoft News Centre Europe.* May 28, 2020. https://news.microsoft.com/europe/features/why-we-need-more-diversity-in-cybersecurity/

"Strategies for a Diverse Pipeline." https://scholarworks.iu.edu/dspace/bitstream/handle/2022/21734/StrategiesDiversePipeline.pdf?sequence=2.

"The Snowden Effect." *The Economist*, January 24, 2014. https://www.economist.com/babbage/2014/01/24/the-snowden-effect.

Stewart, Camille. "Systemic Racism Is a Cybersecurity Threat", *Council on Foreign Relations,* June 16, 2020. https://www.cfr.org/blog/systemic-racism-cybersecurity-threat.

Sulmeyer, Michael. "How to Compete in Cyberspace,", *Foreign Affairs,* August 25, 2020. https://www.foreignaffairs.com/articles/united-states/2020-08-25/cybersecurity.

Tapia, Andrea H, and Lynette Kvasny. "Recruitment Is Never Enough: Retention of Women and Minorities in the IT Workplace", *Proceedings of the 2004 SIGMIS Conference on Computer Personnel Research, Tucson, AZ*, 2004. https://pennstate.pure.elsevier.com/en/publications/recruitment-is-never-enough-retention-of-women-and-minorities-in-/fingerprints/

Tiku, N.,. "Google's Approach to Historically Black Schools Helps Explain Why There are Few Black Engineers in Big Tech", *Washington Post,* March 4, 2021.

Troianovski, Anton. "WikiLeaks Plans Publishing Documents 'Significant' to U.S. Election." *Wall Street Journal*, October 4, 2016, sec. World. https://www.wsj.com/articles/wikileaks-plans-publishing-documents-significant-to-u-s-election-1475576676.

Twersky, F., "The Listening Post", *Hewlett Foundation,* November 2, 2020. https://hewlett.org/the-listening-post/

"U.S. Cyber Command History." *U.S. Cyber Command.* https://www.cybercom.mil/About/History/.

The U.S. Secretary of Commerce and the U.S. Secretary of Homeland Security, "A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future", Washington, DC, May 2018. https://www.nist.gov/sites/default/files/documents/2018/07/24/eo_wf_report_to_potus.pdf.

Van Horn, Carl E., ed. "Investing in America's Workforce: Improving Outcomes for Workers and Employers". *Upjohn Institute for Employment Research*, 2018.

Van Zadelhoff, M., "Cybersecurity Has a Serious Talent Shortage. Here's How to Fix It." *Harvard Business Review*, May 4, 2017. https://hbr.org/2017/05/cybersecurity-has-a-serious-talent-shortage-heres-how-to-fix-it.

"2017 Global Information Security Workforce Study: Women in Cybersecurity", *Frost and Sullivan,* 2017. https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/wp-content/uploads/2019/01/women-cybersecurity-11-percent.pdf