Findings from the Hewlett Cyber Initiative Summative Evaluation

OCTOBER 2023

Prepared for
The William & Flora Hewlett Foundation

Prepared by
Informing Change

INFORMING CHANGE

Acknowledgments

This report would not have been possible without the input and participation from a range of experts across cyber policy and philanthropic fields. We would like to extend our deepest gratitude to the many individuals who contributed to this body of work via interviews, feedback on data collection tools, report drafts, and vignettes, and who helped guide the evaluation to ensure its results would be relevant and meaningful, including:

- **Initiative Grantees** (unnamed to protect interviewee confidentiality)
- **Non-Grantee Experts in the Cyber Policy Field** (unnamed to protect interviewee confidentiality)
- **Hewlett Foundation Peer Funders** (unnamed to protect interviewee confidentiality)
- **Cyber Initiative Consultants and Partners:** Michael D. Rubin & Associates, 15-Minutes Group, Glenn Echo, Camber Collective
- **Advisory Committee Members:**
  - Frédérick Douzet, Professor of Geopolitics at the French Institute of Geopolitics (University of Paris 8), Director of the Center Geopolitics of the Datasphere (GEODE);
  - Jamil Jaffer, Assistant Professor of Law at George Mason University; Founder and Executive Director, National Security Institute; Director, National Security Law & Policy Program
  - George Perkovich, Ken Olivier and Angela Nomellini Chair Vice President for Studies at Carnegie Endowment for International Peace (CEIP)
  - Monica Ruiz, Program Manager, Senior Government Affairs Manager, Digital Diplomacy, Microsoft
  - Megan Stifel, Chief Strategy Officer for the Institute for Security and Technology (IST)
  - Steve Weber, Founding Faculty Director of the Center for Long-Term Cybersecurity (CLTC) at UC Berkeley
  - Benjamin Wittes, Lawfare Editor in Chief; Senior Fellow in Governance Studies at the Brookings Institution
- **Hewlett Foundation and Initiative Staff:** Amy Arbreton – Evaluation Officer, Effective Philanthropy Group, Kelly Born – former Initiative Director, Sherry Huang – Program Fellow, Larry Kramer - President, Leanne Oue – Grants Officer, Eli Sugarman – Initiative Director, Kristy Bernard Tsadick – Deputy General Counsel, Heath Wickline - Deputy Director of Communications, Marlene Zapata – Program Associate

Their collective input contributed invaluable wisdom to this evaluation.

Table of Contents

THIS REPORT WAS PREPARED BY:

- AnnJanette Rosga, PhD – Director, Informing Change
- Elidé Flores-Medel – Founder & Principal, Meaningful Observations
- Evan Gattozzi – Senior Associate, Informing Change
- Rachel Kramer, MIDS – Associate, Informing Change
- Johnny Du – Writer/Editor, Informing Change
- Emily Medica – Research Assistant, Informing Change
- Inti Chomsky – Associate, Informing Change
- David Shin – Research Assistant, Informing Change

INTRODUCTION

The Big Bold Goal: Developing a Field of Cyber Policy Experts

In 2014, the William & Flora Hewlett Foundation (**the Foundation**) created the Cyber Initiative (**the Initiative**) with the objective of **establishing a cyber field of multidisciplinary**[1] **experts with the necessary knowledge, expertise, and reach to inform policymakers and the public about pressing cyber issues**. The Initiative was originally intended to invest a total of $20 million over a five-year period, with an additional $45 million investment in three core academic institutions to support one of three key strategies. In 2017, with a clearer understanding of the need and potential for impact in the cyber field, Hewlett extended the Initiative an additional five years (through 2023) and increased its budget. As of August 2023, the Cyber Initiative has invested more than **$163.6 million through grants and contracts.** This total includes grants made through the Cyber Initiative, Organizational Effectiveness (**OE**) grants made to numerous Initiative grantees, and Direct Charitable Activity (**DCA**) contracts to support Initiative events and other training or technical assistance.

Why This Initiative?

Soon after being named President of the Foundation in 2012, Larry Kramer set out to identify a new area of grantmaking. Given the Foundation's Nuclear Security Initiative was sunsetting in 2014, Kramer began considering what security-related horizon Hewlett could explore next. Drawing upon his own knowledge of cybersecurity garnered while at Stanford Law School,[2] he asked a small team at Hewlett to spend a year researching the state of play in cybersecurity. They conducted more than 60 interviews with experts across a range of cyber-related sectors and disciplines. Three key gaps impeding the creation of strategy-driven and evidence-informed cybersecurity public policy emerged from this research; the team proposed to the Foundation's board three corresponding ways the Foundation could contribute meaningfully to addressing these gaps:

1

Gap: The government and private industry invested heavily in cybersecurity but without a clear framework or governance plan. This reactive approach limited holistic and strategic policy thinking about how to deal with cyber threats.

Opportunity: Carve more intentional paths forward for the field across industry and the public sector.

2

Gap: While individuals with expertise in technology (tech) or policy existed, few, if any, held expertise in both areas, resulting in a lack of multidisciplinary knowledge to support the future of the field.

Opportunity: Support and develop institutions to help equip individuals with the necessary knowledge and expertise in both cyber policy and tech to inform decision-makers and the public.

3

Gap: Those few individuals with both sufficient technological understanding and skills, interest, and networks to effectively inform public policy lacked a cohesive, collaborative community in which to develop shared vocabularies and priorities. In some cases, there appeared to be animosity or distrust between communities of technology experts and those of policy experts.[3]

Opportunity: Create spaces for trust-building among experts to help bridge the gap between siloed disciplines and communities.

Hewlett concluded in sum that, despite the presence and expressed interest of many experts, a shared "field" did not exist yet. That is, a "field" capable of meeting the research and information needs of policymakers being outpaced by the corporate-dominated cybertechnology sector while helping the public understand and contribute to cyber policy debates. These circumstances allowed Hewlett to exercise one of its unique strengths: grantmaking in the service of field building. In keeping with Foundation practice, the Cyber Initiative's work is "not focused on field building for its own sake, but rather, as the best way to generate improved policy decisions."[4]

> "The idea of filling the gaps in what government and industry were doing was obviously important. They were putting out daily fires but not really dealing with the long-term framework needed to prevent those fires or keep them controlled. To me, it was a cyber policy initiative that would help government and industry do better."
>
> – HEWLETT FOUNDATION PRESIDENT LARRY KRAMER

THE FOUNDATION'S APPROACH TO FIELD BUILDING

Hewlett is one of only a few philanthropic institutions that have made field building a central grantmaking strategy, and it may be one of the Foundation's most well-known and impactful ways of investing in the social sector. Although Hewlett does not have a uniform approach to creating coordinated portfolios of grants to multiple organizations within specific arenas, we can discern a handful of similarities across its programs with field-wide foci. Many of these programs, both current and past, have set out to:

- Nurture organizational ecosystems;
- Support diverse pipelines and networks of actors;
- Encourage collaboration and communication;
- Facilitate learning; and
- Encourage evidence-based problem-solving.

Where field building is the central goal, the Foundation has identified contexts in which fragmentation exists among approaches, or where ideas, solutions to complex social problems, and organizations are just beginning to emerge—especially in public policy or policymaking processes.

Brief History of the Cyber Initiative & Its Evolution

At the Initiative's outset, Hewlett grappled with a few key questions, including:

- What to call the Initiative given the breadth of subfields it could touch;
- How to address the need for a robust academic field focused specifically on cyber issues; and
- The challenges of communicating complex issues to non-experts who would benefit from the information.

Though the initial exploration of the subject was inspired by cybersecurity, and because it wasn't yet clear the focus would be largely on cyber policy, Hewlett ultimately opted for a broad framing, calling its new portfolio the **Cyber Initiative**. Though this more expansive name came with its own set of limitations, it provided flexibility and appeal, allowing for more potential grantees to see themselves as part of the work and to continue to focus on their areas of expertise in cyber-related subfields. The Foundation also understood creating an entire academic field on its own would be prohibitively expensive, so it sought to leverage key established institutions instead. Kramer hypothesized selecting elite universities where cyber-related scholarship was already occurring would motivate other universities to emulate these universities by creating new cyber-focused academic programs of their own.[5] Hewlett looked to these investments to "anchor" the Initiative in the field, wagering multimillion-dollar grants on their reputations, likelihood to succeed, and potential to inspire other institutions. Finally, Hewlett also leveraged the media and engaged journalists to help develop information-sharing infrastructure that could support the distribution of compelling, well-informed, and comprehensible-to-general-reader stories about cyber policy-related matters.

WHAT COUNTS AS "CYBER"?

In 2014, the Hewlett Foundation named its new effort, focused heavily on cyber policy, the "Cyber Initiative."

The Foundation used a broad definition of cyber policy "not only to include 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." It also included areas that many conceive of as "tech" and "digital" policy.*

Hewlett's goal was to create an intentionally broad space so that grantees could continue their existing work and grow the field over the course of the Initiative. However, many cyber policy practitioners use different definitions of "cyber" in their own work. This tension is described more fully in the "What's in a Name?" callout box on page 15.

—

*Camber Collective. (2022). *Grantee Survey – 2023: For Calendar Year 2022*. Unpublished survey protocol.

Hewlett refined its approach during its first few years to solidify the three core pillars of the Cyber Initiative: supporting the development and sustainability of (1) strong institutions, (2) a talent pipeline, and (3) a translation and communications infrastructure.[6] Threading through all three was a push to ensure the cyber field would be diverse geographically and ideologically, and inclusive of more women.

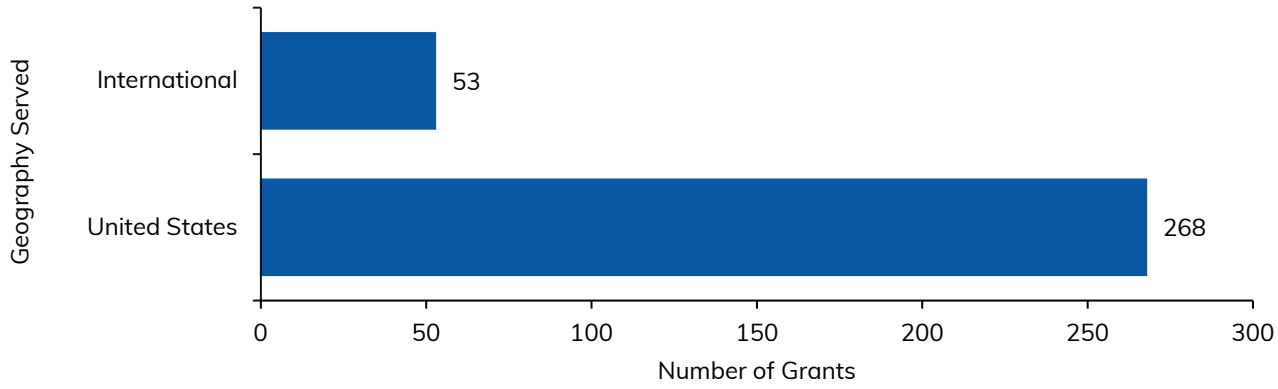
> "We wanted to launch a field, and we knew [academia] would have an important role in that, both because so much research is done in universities and because that's where people get their training. But we couldn't fund every university ourselves, or even a great many of them; it would have been much too expensive. Instead, we thought, 'If we can pick the right schools to begin with, it will generate competition, as other universities won't want to just let those first movers have the whole field. Then other universities could and would turn to their own independent sources of funding to get into the game.'"
>
> – HEWLETT FOUNDATION PRESIDENT LARRY KRAMER

The Cyber Initiative by the Numbers

By the time it sunsets, the Cyber Initiative will have invested more than $163 million over its 10-year lifespan. As of August 2023, this includes **268 grants** to **US-serving** organizations and **53 grants** to **international** organizations (**Exhibit 1**).

EXHIBIT 1

Geography Served by Cyber Initiative Grants[7]
(As of August 2023)



INTERNATIONAL FUNDING

Hewlett originally created the Cyber Initiative with a focus on the US. In 2016, the Initiative broadened its portfolio to include some grantees based outside of the US, acknowledging that it is "critical for the Cyber Initiative to have a global outlook given the international dimensions of the Internet and inability of individual countries to tackle cybersecurity challenges alone."* Hewlett prioritized international funding on organizations in "focal" countries so as not to spread its available funding too thinly: they began with India, given its large technology sector and influence in the developing world, and Germany as the "linchpin of Europe and critical to help repair the frayed transatlantic cyber policy discourse."** Hewlett later extended international funding to France and a few other countries, though they noted in 2017 that they did not expect international grants to exceed 10–15% of their annual investments.*** Hewlett points to the work in France and Germany as evidence of the success of the Initiative's international funding. Funding to Université Paris 8 (three grants totaling $850,000) supported the Geopolitics of the Datasphere (**GEODE**) Center, a multidisciplinary research and training center, which has been awarded a "Center of Excellence" label by the French Ministry of the Armed Forces as part of the Higher Education Pact (we explore the Higher Education Pact more deeply in the vignette on page 18).† Funding to Stiftung Nueu Verantwortung (**SNV**), a think tank in Berlin aimed to sustain SNV as a core institution for European and transatlantic cybersecurity policy research and collaboration. Seven grants totaling $1,539,000 supported SNV's work, including their work on the Transatlantic Forum for Cyber Policy, an intersectoral network of more than 150 experts from civil society, academia, and the private sector.

–

* Hewlett Foundation. (2015, September 16). Program Budget Memo: Cyber Initiative. Unpublished internal document.

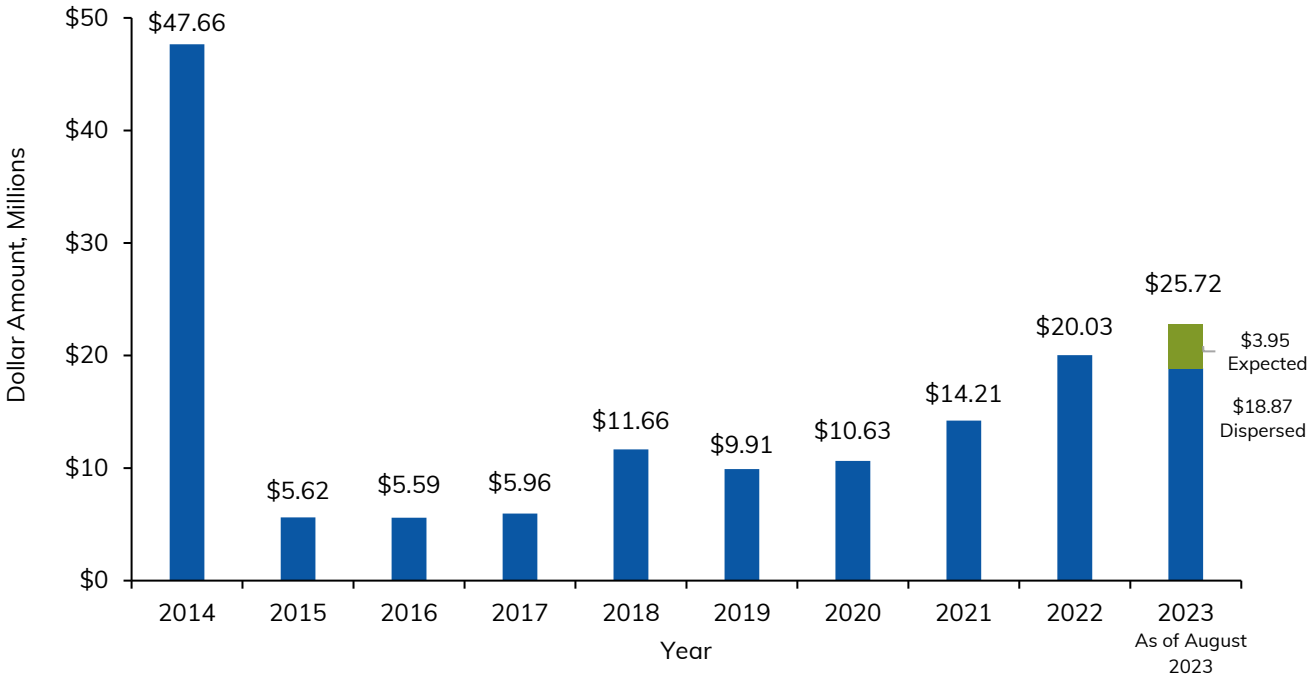
** Hewlett Foundation. (2016). Program Budget Memo: Cyber Initiative. Unpublished internal document.

*** Hewlett Foundation. (2017, October 16). Program Budget Memo: Cyber Initiative. Unpublished internal document.

† The Geode Center. https://geode.science/en/home-2/

Exhibit 2 shows the Initiative funding each year. The amount of funding during the Initiative's first year was substantially higher than in later years due to an initial three $15 million grants (totaling $45 million) to universities. Grant dispersal in 2023 will continue through the end of the year and is expected to total nearly $25.7 million.

EXHIBIT 2
Cyber Initiative Funding by Year
(As of August 2023)



Initiative funding also went toward contracts for Direct Charitable Activities (**DCA**) (e.g., convenings) and organizational effectiveness grants.[8] The DCA and organizational effectiveness totals below reflect what has already been dispersed over the course of the Initiative (through August 2023), as well as what Hewlett expects to grant or contract through the end of 2023.

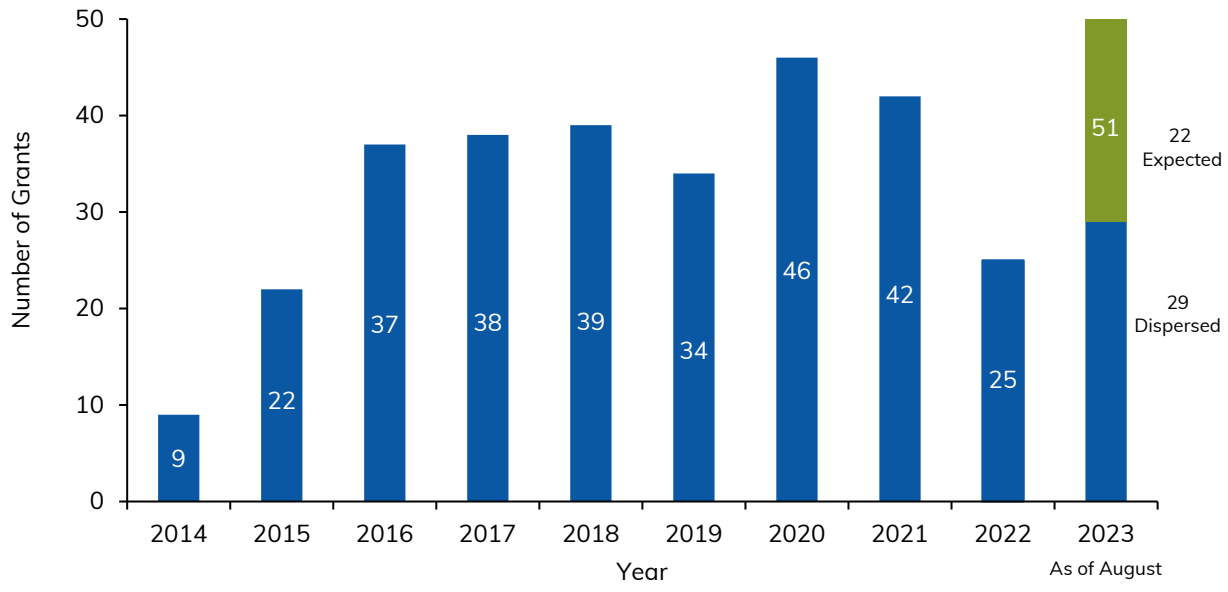
$6.6 million
over 74 contracts
Direct Charitable Activities (DCA)

$1.9 million
over 38 grants
Organizational Effectiveness (OE) Grants

Beginning in its second year, the Cyber Initiative made at least 22 grants annually, with a high of 46 in 2020 that is expected to be exceeded in the final year; final grants will be awarded through the end of 2023 before the Initiative's end (**Exhibit 3**).

EXHIBIT 3

Number of Cyber Initiative Grants Awarded by Year (As of August 2023)



The Cyber Initiative Timeline in Context

For most individuals and organizations in the US, the past 10 years have seen a series of key events profoundly impact the ways and degrees to which our lives are reliant on digital technologies and the vulnerability of these technologies, including the 2016 US presidential election and related cyber and disinformation campaigns, COVID-19 pandemic, and the 2020 murder of George Floyd. These contextual factors heightened attention toward both cyber-related and diversity, equity, and inclusion (**DEI**) issues in the US and globally and left their mark on the Cyber Initiative as well; see the timeline on the next page.

GLOBAL CYBER-RELATED EVENTS	CYBER INITIATIVE TIMELINE
Pre-Initiative Through 2014 Launch	
• Cyberwarfare against **Estonia** destabilizes government and economy **(2007)** • **Sony** PlayStation Network hack **(2011)** • **Edward Snowden** releases classified NSA documents to the public **(2013)** • **Yahoo!** data breach **(2014)** • **Russia destabilizes Ukrainian** computer networks and interferes with Ukraine's presidential elections (initial Russian cyber offense in Ukraine) **(2014)**	• **Hewlett Cyber Initiative launches** as a 5-year Initiative **(2014)** • $15 million **grants to three "anchor grantee" universities (2014)** • **Eli Sugarman** assumes the role of the Cyber Initiative Director **(2014)**
2015–2019	
• **DNC** computer network hack **/ US** presidential election **/ US election interference** and use of social media for misinformation campaigns **(2015/2016)** • EU adopts **General Data Protection Regulation (**GDPR) **(2016;** went into effect **2018)** • **California Consumer Privacy Act (CCPA) signed (2018;** went into effect **2020)**	• First **grantee convening (2016)** • **Strategy refresh**—narrows goals from five to three **(2017)** • Board **extends Cyber Initiative an additional five years**, making it a 10-year Initiative **(2017)** • **Verify**, Hewlett's "first ever high-level media roundtable," is held **(2018)** • Initiative **adds two think tank "anchor grantees,"** R Street and Carnegie Endowment (CEIP) **(2018)** • Initiative sponsors congressional panels and talks at **DEFCON**, the largest hacking conference in the world (~30k attendees) **(2019)** • Two additional **"anchor grantees"** are added (CyberPeace Institute, Georgetown's CSET) **(2019)** • Large grants to **"anchor grantee" university MIT concludes (2019)**
2020–2024	
• **COVID-19 Pandemic** leads to increase in digitization and online activity, as well as an increase in cyber-attacks **(2020)** • Murder of **George Floyd** sparks national reckoning with racism **(2020)** • **Russia invades Ukraine (2022)**	• In partnership with OpenIDEO, Initiative launches the **Cyber Security Visuals Challenge (2020)** • Cyber media roundtable (Verify) and annual grantee convening **cancelled due to COVID-19 (2020)** • **Kelly Born** takes over as Director of Cyber Initiative **(2021)** • **DEI Learning Cohort and grants** to minority serving institutions **(MSIs)** are given as part of DEI efforts **(2022)** • Director **Kelly Born** exits Hewlett and **Eli Sugarman** steps back in to guide Cyber Initiative through its sunset **(2023)** • DEI effort continues through a **new grantee cohort**: Cyber Collective, Govern for America (**G4A**), and Women in Cyber Security (**WiCyS**) (2023) • Final two large grants to **"anchor grantee" universities (UC Berkeley and Stanford) conclude (December 2023)** • **Cyber Initiative Sunsets (December 2023)**

Winding Down the Cyber Initiative

Having learned from the backlash against its quick exit from the nuclear security field, the Foundation was mindful of the need to provide clear messaging about the time-bound Cyber Initiative from the outset. Time-bound initiatives are one way Hewlett creates opportunities to invest in efforts related to "current and timely problems" not otherwise included in its core programs.[9] As such, Hewlett entered the cyber space transparently, stating its intention to fund for a finite period. While Hewlett staff acknowledge the 2017 extension of the Initiative could have caused confusion or given grantees a false sense of hope that the Initiative would not eventually sunset, the Foundation has held firm in its commitment to exit the field eventually.

Because Hewlett intended to build something lasting, Cyber Initiative staff implemented several strategies to help grantees prepare for the Foundation's eventual departure. For example, they implemented a soft fundraising match requirement to encourage grantees to seek other sources of support, connected them to other potential funders, provided grants to build their organizational capacity (i.e., Organizational Effectiveness grants), and hired fundraising and communications consultants to work with grantees on their development efforts and to understand the fundraising landscape.

> "I feel like we've done something with [Hewlett's] grant funding we would not have otherwise done, which I think has resulted in a contribution to public debate in policy that's valuable … We have been able to do some really cool stuff because of [the Initiative] and actually create something sustainable that will outlast the Initiative … That's kind of the dream outcome for that sort of funding … We're off and we're running."
>
> – GRANTEE

Evaluating the Cyber Initiative

Evaluation and learning are integrated practices at Hewlett, used to support data-driven decisions. Hewlett commissioned research, evaluation, and other data-focused projects throughout the Cyber Initiative to help inform decisions about its direction and development.

In summer 2022, the Foundation commissioned Informing Change, a strategic learning firm based in Berkeley, CA, to conduct a final summative evaluation of the Cyber Initiative. Hewlett wanted to understand the Initiative's evolution and how the decisions Hewlett staff made throughout the Initiative influenced and affected its outcomes and its overall results. Because so much information had already been collected, the Foundation agreed we should focus our efforts on an in-depth review and synthesis of prior (often quantitative) data, supplementing this with new qualitative data collection.[10]

Informing Change engaged an Advisory Committee comprised of six Initiative grantees and field experts to help guide the evaluation and ensure clarity and relevance to multiple audiences. Advisory Committee members provided input on the evaluation plan, evaluation questions, and interview protocols.

Based on questions Hewlett articulated in the evaluation's original Request for Proposals, and with Advisory Committee input, Informing Change developed the following high-level evaluation questions:[11]

1. To what extent, and in what ways, did the Initiative achieve its goal of cultivating a multi-disciplinary cyber policy field of institutions to which decision-makers can turn, and in which they and the public may place justified confidence?

2. What contributed to the Initiative's successes, and what factors inhibited or thwarted success?

3. How, and to what extent, did the Initiative contribute to elevating the profile and visibility of cyber topics and concerns in the media and the general public discourse?

4. What lessons learned through the Initiative might inform the Foundation's other grantmaking and/or other funders' choices and grantmaking processes?

As our data collection and analysis evolved, we realized that organizing our reporting by evaluation question would require excess repetition of key points. Hence, we elected to tell the story of the Initiative according to its focal areas and goals instead. **See Appendix D for a full list of evaluation questions and succinct answers to each of them.**

This summative evaluation used a mixed-methods approach, including:

1. **Desk Review**. A systematic review of existing documents including internal strategy articulations, board memos and reports, previously commissioned evaluation reports and field scans, and data collected to date via a Camber Collective annual grantee survey and field expert surveys. The full list of reports, research, and evaluations commissioned or developed throughout the Cyber Initiative reviewed as part of this summative evaluation can be found in **Appendix B**. We also analyzed data from Hewlett's Salesforce grants database to understand the scope of funding, grant amounts and totals, and other quantitative outputs.

2. **Interviews**. A series of original interviews with four stakeholder groups: (1) Foundation staff and Initiative consultants, (2) Initiative grantees, (3) field experts, and (4) select staff from other foundations (or other funders) with current, previous, or potential investments in the cyber field. Informing Change conducted a total of **44 interviews with 46 individuals** to supplement existing data. Interviews included:

    - **8 Foundation Staff**: To understand Hewlett staff's own assessment of progress, challenges, and learnings, including the key assumptions undergirding the Initiative's approach, its pivots over time, and what other funders might learn from Hewlett's experience.
    - **21 Representatives from 20 Initiative Grantees**: To explore the changes that have occurred through or resulting from grantees' work, the Foundation's contributions to these changes, as well as contextual factors and reflections on the Initiative and its approach.
    - **8 Field Experts**: To establish a broad and strategic view of the cyber policy landscape and what may be on the horizon, with insights from cyber industry professionals, journalists/reporters on the "cyber beat," and academics who could speak knowledgeably about the topic.
    - **4 Representatives from Hewlett's Peer Foundations**: To explore the perspectives of staff from current and previous funders in the field on opportunities and challenges to funding in this space.
    - **5 Consultants to the Initiative** (in 4 interviews): To understand the services and support consultants provided to grantees, the consultants' perspectives on the successes and outcomes of their work, and what funders, including Hewlett, can learn from their experiences.

3. A brief set of **survey questions** was added to Camber Collective's 2023 annual grantee survey. In total, **42 grantees responded to the survey**.

Informing Change representatives also attended the November 2022 grantee convening to answer questions about the evaluation, discuss policy advocacy evaluation strategies and methods, and learn about the Initiative. We provide more details about our evaluation approach, methods, and data collection tools in **Appendix E**.

Evaluation Limitations

We note four key limitations to this evaluation:

1. Testing the degree to which the Initiative can *alone* be credited with changes in the cyber field is beyond the scope of this evaluation. The field greatly expanded and evolved during the Initiative's active period and was subject to the influence of innumerable external factors. The findings and recommendations in this report are reflective of triangulated research drawn from annual survey data, interim evaluation and other reports, and our own extensive interviews with a variety of field experts and others familiar with the Initiative. We therefore have confidence in the findings reported here and in the overall claim that Hewlett's investments have catalyzed and significantly contributed to the cyber field.

2. The Cyber Initiative's strategy was substantially revised once the Initiative was underway, as Foundation staff learned more about the needs of grantees and the field. While this nimble approach enabled the Initiative and its grantees to shift and evolve as needed, it did not allow for comparison of a fixed set of indicators from start to finish.

3. The majority of perspectives informing this evaluation represent a US-centered (and to some degree Western-centered), rather than a global lens, due to the fact that most Cyber Initiative grantees are based in the US and US-serving.

4. There is no universally accepted definition of the "cyber field" that satisfies all parties participating in this evaluation; their distinct backgrounds and experiences influence the lenses through which they define the field. However, it is worth noting that even members of very well-established multi-, inter-, and trans-disciplinary fields find themselves disagreeing frequently on the purpose, content, and boundaries of those fields. When we describe the "field" in this report, it is limited to Hewlett's broad definition (see the callout box on page 3 of this report), which may differ from how other entities define it or use the term in practice.

Report Structure

The remainder of this report is organized by overarching topical and thematic findings. When possible, we organize findings by Initiative strategy. As noted above, we elected to use findings to structure the report rather than evaluation questions as interviewees' answers to these questions frequently overlapped, making it difficult to adhere to the structure without duplicating findings. We provide concise answers to evaluation questions in **Appendix D**. The report is structured as follows:

- Findings related to Initiative strategies,
- A discussion of Diversity, Equity, and Inclusion (DEI) in the Initiative and the field, more broadly,
- A description of the cyber policy field today as Hewlett exits the field, and
- Lessons learned from the Initiative and how funders interested in the field can apply them.

FINDINGS

Hewlett Foundation's Cyber Initiative: Both Leading & Following the Field

The cyber policy field has evolved significantly since Hewlett launched the Cyber Initiative. Interviewees describe the pre-Initiative cyber field as being small, siloed with niche sub-fields, and having significant knowledge gaps. There were few nonprofits in the space, as most cyber work was government-led and related to national security, which meant security clearance was required to work with the government. There was a major deficiency of multidisciplinary knowledge, with experts on the technical side of cyber who did not understand the policy side, those with policy expertise lacking proficiency in relevant technical matters, and very few experts or leaders who had deep knowledge in both areas. There were few-to-no cohesive connections, nor a shared language across various sub-fields within cyber.

Hewlett chose to enter a field still in its nascent stages; it was largely ad hoc, without many dedicated cyber programs, either in higher education or other entities. Those programs that existed pre-Initiative often made do with barebones staff and minimal resources. **While the field has evolved significantly over the past decade, how much did the Initiative's field building efforts contribute to this evolution?** As one Hewlett staff member put it, "Were we riding the wave or generating the wave?"

Foundation staff believe they were likely *both* riding and generating the wave, simultaneously. While a definitive answer to that question is not possible given multiple confounding contextual forces, **we found general agreement among interviewees that Hewlett was consistently successful at meeting the needs of the moment**, bringing resources to the few organizations active in the space, anticipating future needs by helping to build up a talent pipeline of future workforce expertise, and establishing and supporting civil society organizations that could respond to the needs of the cyber field.

Elevating the Field's Visibility

The most pronounced change identified by those who spoke with Informing Change is an increase in awareness of cyber as a set of problems and issues that need to be addressed. Previously, awareness of cyber security threats was primarily among corporations and governments, but members of the public are now increasingly conscious of the fact that they, too, can be directly affected by cyberattacks.

> "Ten years ago, the pockets of cyber policy that existed were niche, highly government-led, closed-door, and secret as a result. There were hardly any nonprofits active in cybersecurity. We've seen the democratization of this topic, moving it out of the realm of only being a national security conversation and talking instead about the impacts and relevance on people's daily lives, talking about cybercrime, which has become such a massive issue, and you see a much greater level of accessibility."
>
> – FIELD EXPERT

Private industry and government parties are far more aware of these risks than ever before; one interviewee noted that, in 2012, the Obama administration had to be convinced cybersecurity was a national problem.[12] Now, the dangers of cyber vulnerabilities are accepted and policymakers no longer have to justify spending

taxpayer money on cyber issues, as evidenced by the number of government units dedicated to working on various cyber issues.[13]

Many cybersecurity companies have built out research departments, adding in-house cyber expertise for their products, as well as educating their customer base through white papers and other publications. Multiple interviewees brought up the 2016 US presidential election as an inflection point in public and government awareness that cybersecurity affects a wide range of stakeholders, including industry, government, and the public.[14] Interviewees also spoke about a higher demand for cyber knowledge, largely because of increased cybersecurity breaches, as another sign of field maturity, but this demand predominates in technical settings.

There is more applied policy research, higher quality research overall, and more translation of academic research into language that policymakers can understand. There is also increased demand from the press for cyber aptitude, as evidenced by the larger set of cyber professionals whom journalists interview.[15]

Over the course of the Initiative, the cyber field has seen an increase in the amount of cyberspace regulation, both through government mandates and the formulation of voluntary standards across various cyber domains. This includes *The UN Norms of Responsible State Behaviour in Cyberspace*, [16] various sets of suggested AI standards (including standards meant to protect human rights), and the National Institute of Standards cybersecurity framework. One expert noted the emergence of a need for digital infrastructure standards but said there is disagreement in the field over whether those standards should be government- or industry-led. Government entities—at least in the US, EU, and India, where our interviewees were most knowledgeable about government bodies—have grown significantly in their capacity to understand cyber issues. Another expert noted the increase in the number of qualified cyber professionals was apparent during the search for a National Cyber Director (a federal government position established in 2021). However, grantees also pointed out that the way technology has developed has often prioritized the existence of, and access to, technology over how it might be used or with sufficient attention to the vulnerabilities it may have.

> "Technology has developed in a very freedom-centric way which, taken to its extreme, has meant it created a certain kind of cyber ecosystem which some people around the world have objected to because it is permissive of lots of kinds of content that people find objectionable. That's part of the US attitude and Silicon Valley ethos."
>
> – FIELD EXPERT

The EU has been more willing to regulate cyber technology, passing the General Data Protection Regulation (**GDPR**) in 2016, which multiple interviewees saw as a sign of field-level progress, despite US reluctance to pass an equivalent law in full.[17] Interviewees noted many countries or companies blatantly violate the voluntary standards described in the preceding paragraph, even when the standards are broadly accepted. One of Hewlett's peer funders said companies often use voluntary ethical standards to avoid accountability for harms they produce (e.g., through products put to market with significant security vulnerabilities, tracking and sale of consumer information, decision-making technologies that operate with various biases, and unclear or undisclosed policies permitting information-sharing with law enforcement or government bodies).

Overall, **interviewees describe the current cyber field as more organized, focused, and better documented than it was before the Cyber Initiative**. **They also said threats are easier to articulate, with more mature conversations occurring on specific issues** (e.g., encryption backdoors, export controls, vulnerability research, and offensive tools) **and more advanced tools and frameworks available** to help address cybersecurity issues. There is more collaboration and coordination between government entities and an increase in how multidisciplinary the field is.

Hewlett's Contribution to the Growth & Coalescence of the Cyber Policy Field

Grantees, experts, and peer funders variously described **Hewlett's primary contribution as supporting, shaping, accelerating, and adding intentionality to the growth of the cyber field**. Interviewees view the Initiative's role in ways that align with Hewlett's vision of field building: Hewlett had no specific policy or issue goals in mind but sought to help the field develop in a manner that would close the gaps Kramer and the Hewlett team identified when the Initiative was created, bridging deep silos between issue areas and between policy and technology, increasing multidisciplinary expertise, and creating the conditions in which cyber issues could be more effectively communicated to policymakers and the general public.

Interviewees acknowledged **it is not feasible to quantify the Initiative's direct impact on the cyber field**. It is simply too difficult to separate the role of Hewlett's funding and support from the ways in which the field was propelled by the rapid development of technology, significant geopolitical events (especially election interferences and increase in cyber events), the 'Zoomification' and digitization of daily life accelerated by the COVID-19 pandemic, and the ongoing war in Ukraine.[18]

Attribution aside, grantees were quick to acknowledge **the Foundation had significant impacts on cyber**, largely by:

1. Choosing to catalyze the field in a horizontal manner by funding organizations working across the cyber domain rather than focusing on specific issues or policy outcomes;
2. Being one of the few funders and largest financial contributors to the space; and
3. Networking and supporting or engaging in other "beyond the grant dollars" activities.

In short, **Hewlett's funding, approach to grantmaking, field building, and networking support added crucial intentionality and coordination to the growth of the cyber field**.

> "Yes, it [the growth of the field] would've happened anyway and, yes, it was a natural process, but Hewlett enabled a response that has been a lot more productive and a lot more open and encompassing and inclusive and I think accelerated an ability to address these issues."
>
> – FIELD EXPERT

Catalyzing the Field via Strategic Philanthropy

The grantees, experts, and peer funders whom Informing Change interviewed spoke to significant narrowing of the gaps Hewlett focused on, even if those gaps persist due to structural challenges outside of Hewlett's capacity to influence (such as the disciplinary biases built into academic promotion requirements).[19] **The Foundation's support was influential and critical to helping close these gaps as much as was feasible through private philanthropy.** As one peer funder put it, Hewlett has worked toward the "creation of systemic assets to solve systemic problems and to create an awareness bridge" between them. These assets include graduates with a multidisciplinary cyber skillset, research by a diverse array of organizations, and communication resources including education for journalists.

The Foundation also supported a talent pipeline emphasizing cross-disciplinary training in policy, technology, and other relevant domains. **By using the bulk of its funding to seed many academic programs, the Initiative contributed to an influx of qualified talent to fill the plethora of vacant roles in various cyber-related jobs across industry, government, and civil society.** Hewlett funding was instrumental in getting myriad degree programs off the ground; according to Camber Collective data, Initiative grantees with academic programs have increased the number of degree offerings[20] and seen a steady rise in both applications and enrollments.[21] Interviewees from academic grantee institutions felt relatively confident in the sustainability of the programs that Hewlett catalyzed, both because they have shown enough success in their work to secure additional funding, and because employers have better grasped the need for a cyber workforce trained across previously siloed disciplines.

The Foundation's support was also instrumental for other civil society organizations, particularly think tanks. This funding helped add a diverse range of new programs and institutions to the field. Camber Collective's 2016 Network Evaluation Report noted the field lacked political diversity at the time.[22] **The Initiative addressed this by funding organizations representing a wider range of political ideologies, particularly by adding right-leaning think tanks to their grantee pool to counter the greater prevalence of left-leaning organizations in the cyber space.** Multiple grantees said this ideological diversity was key to the success of the Initiative, as they appreciated interfacing with people and organizations looking at the same issues from a diversity of perspectives and backgrounds.

Many grantees also praised the flexibility Hewlett grants allowed them. They noted funding from other entities often comes with restrictions, for example, money from corporate funding is often tied to a particular deliverable, while philanthropic funders often have specific aims for the research they are willing to fund. As a result, nonprofit organizations tend to work on research questions they can successfully obtain funding for, rather than the topics in which they have the greatest interest and which are most relevant to the field. By funding with the goal of a more capable and resilient *field*, Hewlett allowed its grantees to invest their time in issues and problem sets best suited to their staff's proficiencies and areas of concentration, giving them the freedom to pivot when necessary, without worrying about a consequent loss of funding. For example, Camber Collective's 2022 survey data showed many grantees shifted their focus to cyber issues related to the war in Ukraine, and that about half of grantees are now working on issues related to AI policy.[23]

> "Hewlett allowed research in uncharted territory, areas people knew existed, but there just wasn't a lot of research and policy behind [them]. I think that was probably one of the more unique outcomes of the Hewlett support across all grantees."
>
> – GRANTEE

The Initiative also reduced fragmentation and silos within the field by, most prominently, hosting or supporting convenings, as well as organizing activities at external conferences. Many grantees discussed the benefits of these convenings, from hearing about the work of representatives of other organizations with different backgrounds or ideologies to opening doors for more collaborations. Convenings also gave grantees a chance to share what they were working on, reducing redundancies and creating more cooperation across various work silos, such as the policy and technology sides of cyber.

> "There just wasn't a lot of discussion and collaboration and cooperation, and there is now, and there are avenues for it. And in part, that's because the Hewlett Initiative has funded people opening those doors and convening those groups. It's still nascent though, incredibly nascent … and we need it to continue to grow and move forward."
>
> – FIELD EXPERT

WHAT'S IN A NAME?

Most interviewees agreed Hewlett's broad definition of "cyber policy" allowed grantees to understand the issues they worked on from a wider range of perspectives, and that research from different but related cyber sub-fields allowed them to better recognize the overlap in their respective projects. Many grantees noted all cyber threats are effectively hybrid threats involving multiple areas within cyber, and that cultivating multiple perspectives from those impacted differently on the same issue was a positive feature of the Initiative. Interviewees also reflected that defining cyber more broadly allowed Hewlett to adapt to changes in the types of research needed to keep up with the swift pace of technology and resulting shifts in cyberspace.

Many interviewees described applying a narrower definition of "cyber policy" within their own work, even as they supported Hewlett's decision to cast a wider net. However, some interviewees offered a more critical perspective of the broad definition; a few remarked that "cyber policy" and "tech policy" are two unique fields with distinct foci and communities, even if some issues overlap and have a shared impact (i.e., a policy impacting cyber would also impact those in tech policy). For example, following the 2016 US presidential election, one grantee noted tech platform issues such as content moderation have effectively been "shoehorned" into cyber because there isn't a clear place for them within other fields. In another interviewee's opinion, a wider "cyber policy" umbrella made sense early on, but the cyber field's evolution over the course of the Initiative meant Hewlett missed an opportunity to prioritize depth over breadth by selecting a few key issues within cyber and funding those more fully.

Outside of the breadth of the definition, a few interviewees noted the choice to call it the Cyber Initiative had implications of its own; 'cyber' has a lot of military and national security connotations, whereas policy is often thought of as only legislative, rather than as inclusive of company- or organization-level policies. A peer funder also thought the potentially esoteric nature of cyber concepts—as opposed to a more accessible word like 'tech'—might be a barrier to other funders recognizing the importance and relevance of cyber to more human-centered issue areas, such as human rights or healthcare.

The Foundation did narrow the range of grantees it funded after its midpoint review revealed some investments were "paying off" (with some grantees showing particular promise, and/or clear potential to, become self-sustaining after Hewlett's departure from the field). However, Cyber Initiative staff did retain their commitment to a broad definition of cyber, as to remain relatively issue-agnostic.

"There's no doubt in my mind the Hewlett Foundation stepping in and putting as much money to work in the space as they did, fundamentally reshaped the way people think about this field. I also think the Hewlett Foundation's funding methodology—and its approach and definition of what they were willing to fund—helpfully forced people in otherwise fairly parochial domains to realize that, in fact, you had to think about these problems more broadly. This, in turn, got researchers, academics, and policy advisors to work through these issues with an appreciation for where there were overlaps and intersections between otherwise potentially divergent topics."

– GRANTEE

Funding Research Institutions & Growing the Talent Pipeline

The Cyber Initiative invested in entities that could make meaningful contributions to the emerging cyber field through research, collaborations, and information exchanges, disseminating findings to policymakers and other influential bodies and producing the next generation of cross-disciplinary experts within a multifaceted field. Our evaluation revealed an impressive degree of progress, along with a few areas where opportunities were missed, or investments were less than fruitful. The Foundation's efforts to seed a bed of research institutions included investments in both academic institutions and think tanks.

Academic Institutions

The Foundation's investments in academic institutions launched the Initiative, beginning in earnest during the Cyber Initiative's first year (2014). Hewlett made one-time grants of $15 million each to **MIT**, **Stanford University**, and **UC Berkeley**, establishing them as the Initiative's "**anchor academic institutions**." These anchor grants formed the centerpiece of Hewlett's goal to create a **talent pipeline** from which future scholars and professionals could emerge, trained in at least two disciplines and able to collaborate on pressing cyber policy research. The only restrictions placed on these grants were that (1) they had to be used to fund the development of a center, major, concentration, or other formal training track in cyber policy, (2) have a physical space for the program, and 3) the academic training to be provided must be multidisciplinary and have a pedagogical element.

Hewlett staff continued to apply and expand the application of the **anchor grantee** concept throughout the Initiative. They selected anchor grantees on the basis of their likelihood to succeed and potential to inspire other institutions. The three original anchor grantees were chosen due to their reputations as elite universities and existing strengths in policy and technology. The Foundation also saw them as institutions with the necessary infrastructure to leverage additional funding that would sustain their newly established centers and programs; it expected their prestige and quality to inspire other academic institutions to follow by establishing their own centers and programs. The closing bookend to these anchor investments came in 2022–2023 when the Initiative announced four final grants of $5–6 million each to four minority-serving institutions (**MSIs**): Florida International University (**FIU**), which has a majority-Hispanic enrollment in Miami, Florida; Turtle Mountain Community College (**TMCC**), a tribal college in Belcourt, North Dakota; and two historically Black colleges and universities (**HBCUs**): Florida A&M University in Tallahassee, Florida, and Spelman College in Atlanta, Georgia.

One of the Cyber Initiative's stated goals was to increase the curriculum maturity and available educational offerings related to cyber policy. **Overall, interviewees perceive the increase in the creation of formal academic programs—at the certificate, Bachelor, Masters, and PhD levels throughout universities in the US—focused on multidisciplinary cyber policy to be, at least in part, related to the Initiative's investment.** The presence of cyber education at these universities has evolved from "sporadic classes," as noted by Kramer, to having full-fledged degree programs, departments, and research centers. This started with the three anchor academic institutions and has extended into the Hewlett-supported establishment of programs at George Mason University, Georgetown, Harvard, Tufts University, and the University of Texas at Austin, among others. **Cyber programs at these universities have generally experienced upward trends in the number of applications received and students who enroll**,[24] and grantees and experts **attribute the growth and success of the Initiative-funded institutions directly to the Initiative's initial and ongoing investments in universities**. A Hewlett staff representative observed the expectation that other institutions would follow came to fruition during the Initiative, as American University and Texas A&M established cyber programs of their own without Hewlett funding.

> "Most [grantee academic] institutions probably would not have been as inclined to take a risk and start a new program if it was not for them having an initial investment ... What happened was they had, largely speaking, tremendous success. Hopefully, those institutions have seen the value and would continue funding them."
>
> – GRANTEE

> "[The Initiative] has really encouraged the building up of the field of cyber studies. That's the most powerful impact and was most needed."
>
> – GRANTEE

There was confident agreement among many interviewees that established academic centers, programs, and departments will endure following Hewlett's exit from the field because they exist within larger institutions with the infrastructure to help them continue funding their work.

While the larger grants were successful, a line of smaller investments within the talent pipeline strategy did not fare as well due to structural impediments. Hewlett made some grants designed to support untenured scholars with cyber technology expertise but no training in policymaking (law or political science, for the most part), or vice versa, those with policy training but limited knowledge of cyber technology. However, these grantees experienced challenges, such as those facing multidisciplinary scholars when they seek promotion and low demand for explicit cyber policy expertise in academia. Scholars associated with these grants who sought training to address their lack of expertise found themselves unable to get tenure or had difficulty finding cyber policy academic jobs.[25, 26]

> "There is no pipeline for cyber policy experts because the demand for them is so low. There's a huge demand for cybersecurity experts but for cyber policy? No. Nearly everybody that I know that works in cyber policy is on soft money, including me, and I'm very senior in the field. Cyber policy is not a career you go into for long-term job security."
>
> – FIELD EXPERT

UNLOCKING ADDITIONAL FUNDING & RECOGNITION FROM FRANCE'S MINISTRY OF THE ARMED FORCES

Frédérick Douzet is one cyber professional who benefited immensely from the Cyber Initiative broadening its portfolio in 2016 to include non-US grantees. Douzet is Professor of Geopolitics at the University of Paris 8, director of the French Institute of Geopolitics research team (IFG Lab), and director of the Center Geopolitics of the Datasphere (GEODE), supported by the University of Paris 8. Hewlett funding was instrumental in establishing GEODE via a three-year, $600,000 award to the University of Paris 8 in 2019 to "support the consolidation of a new academic multidisciplinary research center … and the university's graduate program in cyber strategy and data science." The initial award was followed up with one additional award totaling $200,000.

Douzet initially connected with Initiative Director Eli Sugarman at a 2017 conference. At the time, Douzet was providing cyber expertise to France's Ministry of the Armed Forces (then known as the Ministry of Defence) and participating in a competitive process to receive recognition from the Ministry as a 'Center of Excellence.' After being chosen to advance to the final step of the process, Douzet reconnected with Sugarman and the Initiative with her proposal to establish GEODE. The discussions resulted in Hewlett backing GEODE's creation through Initiative funding and supporting the Ministry of Defence application.

Then, in January 2021, GEODE was selected by the Ministry of the Armed Forces as a Center of Excellence for International Relations and Strategy and received a five-year funding award. Douzet believes the Cyber Initiative support "was definitely critical in getting the … Center of Excellence [award]," adding that "maybe we would still have won the competition … but the [Hewlett] grant really provided us the edge."

Today, under a single umbrella, GEODE brings together approximately 40 previously-siloed researchers and doctoral students working on cyber issues in different disciplines (e.g., geographers, computer scientists, mathematicians) at different universities throughout France. Receiving a multi-year commitment from the Initiative allowed Douzet and the GEODE team to concentrate on building up the center without having to spend as much time and resources on fundraising. Douzet appreciated having this peace of mind for such an extended period; to the best of her knowledge, it would be difficult to find a French funding source (e.g., foundation, research agency, or private sector) that would fund as large an amount as what Hewlett offered, and to do so without restrictions on the use of funding, requiring specific target outcomes, or both. Douzet was grateful for the implied trust and lack of micromanagement, remarking, "Nowhere else have I found a grant that gives me money to do what I already do … and trust[s] me to know better than them what should be done."

Douzet believes GEODE is set up well for Hewlett's impending exit and anticipates a renewal of the Center of Excellence funding when it expires at the end of 2025. She praises what Hewlett has done for the field, saying the Foundation "can pride itself in helping build the [cyber] field in France, definitely."

In the Foundation's original vision for the Cyber Initiative, academic programs were to produce interdisciplinary experts to fill cyber policy jobs. Grantee interviewees agreed that, **despite some structural challenges, Hewlett's investments in academic institutions, including MSIs, are leaving the talent pipeline in a much stronger place than it was pre-Initiative**. Increased enrollments have led to more graduates annually, reduced the gaps in personnel qualified for cyber policy jobs, and created and supported a diversity of perspectives informing the field.

> "The need to continue to build the [talent] pipeline and help people actually get jobs is something that could use more emphasis. But there's definitely a cyber pipeline I didn't use to see."
>
> – FIELD EXPERT

> "[I] didn't even know [universities for indigenous Americans were] a thing until I went to a convening and found out Hewlett was providing money to make that happen … My initial reaction [was] 'The investments they had in that area were really important because they brought a lot of new communities in, and I'm not sure that would've happened if it hadn't been for the Hewlett money.'"
>
> – FIELD EXPERT

Some grantees and other experts regarded **curated fellowship opportunities at academic institutions as strategic ways to further reduce the gaps in personnel qualified for cyber policy jobs** with funding to be supplied by tech companies or new funders in the space. Even with higher-paying industry jobs luring away qualified job seekers from civil or government service, **Initiative grantees report substantial growth in the placement of graduates into US-based government positions**.[27] One grantee says the pipeline work has been successful at placing individuals in government or cyber organization roles, and that any gaps in worker supply are not solely Hewlett's responsibility to address.[28] Interviewees named a few specific examples of individuals who have progressed through the pipeline flowing between think tanks, government, and academia, including some individuals from grantee or former grantee organizations, e.g., the Deputy Assistant Secretary of Defense for Cyber Policy, the Deputy National Cyber Director for Technology & Ecosystem for The White House, the Former Senior Director, Cybersecurity Policy, National Security Council (Obama and Trump Administrations), among others. These individuals take the interdisciplinary approach championed by the Initiative. It is too early to fully assess the success of the Initiative's fellowship-funding tactics, however, since they began in the second half of the Initiative.

NATIONAL SECURITY INITIATIVE LEVERAGES HEWLETT FUNDING & "BEYOND-THE-GRANT-DOLLARS" SUPPORT TO LAUNCH NATION'S FIRST LLM PROGRAM IN CYBER, INTELLIGENCE, & NATIONAL SECURITY LAW

In 2011, a few years before the Hewlett Foundation established the Cyber Initiative, the George Mason University (GMU) School of Law had begun addressing a gap in national security law similar to ones Hewlett sought to close; namely that aspiring lawyers in this relatively new and critically important field were disconnected from other practitioners—particularly academics– and faced challenges effectively shaping policy outcomes. The law school's efforts began with a class on surveillance law addressing both legal and technological issues that had driven major policy change in the space, a deliberate effort to establish more classes like these in related areas, and the establishment of the National Security Institute (NSI) in 2017 within what was then renamed the Antonin Scalia Law School.

As NSI created more new opportunities for technologists, policymakers, lawyers, and practitioners to interact, inform, and educate, Hewlett was doubling down on its efforts to catalyze the cyber field by committing additional funding to the effort, including to the NSI. Hewlett initially funded a technology and policy skills translation program for which NSI identified two dozen technologists from around the country who wanted to learn how to influence and inform policy. The program took them through a year-long curriculum to develop the skills to do just that. Over time, Hewlett's support to NSI expanded to general operations funding and was a key element NSI leveraged when it went through a major effort to create the nation's first-ever post-graduate, cross-disciplinary, LLM program in Cyber, Intelligence, and National Security Law.

Without Hewlett's support and guidance, and the expertise that other grantees shared with NSI, there is little chance NSI could have established a graduate degree program. Even as the Cyber Initiative winds down, Hewlett's support is at the heart of NSI's efforts to establish a new Cyber and Tech Center to house the LLM program, similar specializations in Scalia Law's JD and JM programs, and NSI's expanded work in technological innovation and national security. It is precisely because Hewlett leadership had the foresight and patience to commit funding in ways that, at the time, were non-traditional, that NSI was able to establish an academic program and a new center that together continue to grow the cyber workforce and policy conversations in a manner that benefits economic and national security.*

–

* Submitted by Jamil Jaffer, Assistant Professor of Law at George Mason University; Founder and Executive Director, NSI; Director, National Security Law & Policy Program of NSI. Edited by Informing Change.

Think Tanks

While grants to think tanks have been a constant in the Initiative from day one, the Initiative's renewal in 2017 saw an intentional narrowing of scope to provide a deeper level of financial support to a smaller number of organizations. After first trying a "spread bets" distribution of $250,000 awards to a wide variety of think tanks, an approach common to Hewlett's grantmaking efforts, Initiative staff found that few of the (often very small) entities were able to submit promising proposals. Thus, in 2018 staff tried an approach similar to what was clearly picking up steam with most of their large academic investments: to "build a cadre of anchor institutions in the policy development space by making larger, longer, and more flexible grants to a smaller number of grantees."[29] At the time this evaluation began in 2022, **anchor think tanks** included the Carnegie Endowment for International Peace, R Street Institute, the Center for Security and Emerging Technology at Georgetown University, and the CyberPeace Institute.[30]

These and other Initiative-funded think tanks have made impacts both in the talent pipeline and in communications infrastructure, hired and supported Fellows to fill the pipeline, and researched emerging cyber developments like AI and machine learning. They have also published reports and research findings to inform the public and policymakers and collaborated with peers to form taskforces and workgroups for greater influence.

There is general agreement that more people and organizations, particularly think tanks, are focused on cyber issues than before the Initiative. Hewlett funding has provided support for think tanks to hire staff and focus on evolving and pressing cyber needs. Grantees and experts talk about how Initiative funding directly seeded or otherwise helped to create new organizations or new departments with a cyber focus. Grantees have also been able to leverage the Foundation's seal of approval into additional funding. One consultant described the network of think tanks and nonprofits as "much more robust" than it was prior to Hewlett's Cyber Initiative.

Think tanks have also informed and helped shape public policy indirectly through congressional testimony, their research, participation in conferences, and other policy-related meetings. They also train researchers, some of whom go on to hold positions in government.

THE TENUOUS NATURE OF FUNDING THINK TANKS—HIGH RISK, POTENTIALLY HIGH REWARD

Operating with fewer staff and institutional resources than universities or established organizations, newer think tanks lack the donor, alumni, and advocate networks that support colleges and universities. This makes it especially challenging for newer think tanks to sustain their ongoing work. Nonetheless, the philanthropic and private sector funding upon which think tanks rely can also be uniquely valuable in advancing the cyber policy field.

Perhaps no grantee epitomizes this value like The Institute for Security and Technology (**IST**), which received nine Initiative grants totaling nearly $3.3 million, a portion of which was dedicated to supporting the growth and implementation of IST's Ransomware Task Force (**RTF**). This task force brought together dozens of experts from across several cyber siloes (e.g., industry, government, law enforcement) to produce a comprehensive ransomware mitigation framework. IST is currently in the process of implementing recommendations based on this framework.

Michael Rubin, whose consulting practice (Michael D. Rubin & Associates) was engaged by Hewlett to help Initiative grantees build fundraising capacity, named IST as a major success story. Senior Vice President Wendy Rosenblum worked closely with IST staff to instill a culture of philanthropy throughout the organization, including IST's Board of Directors, and helped develop systems prioritizing fundraising as an ongoing, organizational goal. Rosenblum also helped IST develop a strong case for support and ensure messaging across communication platforms aligned with that case; identify and research prospective funders; and create strategies for donor cultivation and stewardship. Rubin pointed to IST's success in more than doubling its staff during the engagement and increasing contributed revenue more than four-fold in less than five years.

IST Chief Strategy Officer Megan Stifel traces support from Craig Newmark Philanthropies, J. Patrick McGovern Foundation, and the Omidyar Network to introductions made by the Hewlett Foundation, but notes IST's stronger fundraising apparatus likely played a key role in their fundraising success as well. Govind Shivkumar, Director of Responsible Technology at Omidyar Network, described IST's continued existence and growth as a testament to the maturity of the cyber field.

Despite IST's own fundraising successes, Stifel has concerns for the cyber policy field at large upon Hewlett's exit, noting that there is still "a long way to go with making the case that cyber is a field that needs philanthropic monies." Stifel believes fewer civil society actors will survive to keep governments and corporations accountable when Hewlett officially exits the field, limiting the field's trajectory as it evolves: "I'm not optimistic that [the near-absence of civil society funders] will be solved by the time [Hewlett leaves] and that will leave a real funding gap for a lot of nonprofits … it's something that we're very conscious of and anxious about."

A healthy stream of available funding from philanthropic actors would permit grantees to be less reliant on corporate support—a funding source that risks undue influence from companies with their own interests and agendas—to stay afloat. Stifel wondered if Hewlett might be in a position to pivot from completely exiting the field to retaining a presence as a thought leader that can continue impacting the cyber field in ways other than directly funding organizations (e.g., continuing to facilitate introductions, publicly weighing in on issues as they emerge, etc.), a viewpoint at least one other interviewee echoed.

> "There's a substantial base of thought leadership in cybersecurity now from multiple parts of the spectrum and from different angles, both domestically and internationally … There's a lot more capability in the field."
>
> – FIELD EXPERT

However, it is difficult to fully capture the extent of think tank contributions to cyber policy. Much policy information exchange—particularly regarding topics that touch on national or global security issues—happens informally, occurring behind closed doors or in other private conversations.[31] This informality makes evaluating its impact especially challenging.[32]

Translation & Communication Infrastructure

As part of their midpoint Initiative refresh, Hewlett staff established a strategy to ensure that grantees' research was shared with decision-makers and the public in ways that were clear, accurate, and understandable. The strategy supported training for grantees to translate ideas, staffing to help grantees communicate them, as well as outlets through which to share them. This strategy was informed in part by recommendations made by RTI International in its 2017 report, *Understanding Demand for Cyber Policy Resources*, specifically the recommendations centered around increasing education and awareness for policymakers, media, and the public, as well as improving and building the communication and exchange of ideas and research between non-government parties and policymakers.

Some key activities related to advancing this strategy included:

- Ongoing support of think tanks and media outlets to increase the visibility and reach of their contributions to cyber policy discourse (e.g., Aspen Institute, Lawfare, National Security Archive, Observer Research Foundation America, Risky Business).
- Starting in 2018, hosting (and in 2022 beginning to co-host with Aspen Digital), four Verify conferences, which "[brought] together leading journalists with top national security officials, tech industry leaders, and experts from civil society to discuss critical issues in cybersecurity and tech policy more broadly."[33]
- Collaborating with OpenIDEO in addressing deficiencies in cyber imagery and visual storytelling through its Cyber Visuals Challenge and subsequent launch of cybervisuals.org.
- Funding training for journalists to deepen their understanding of cyber and investigative reporting techniques (e.g., Global Investigative Journalism Network, University of Maryland).
- Supporting Atlantic Council's annual Cyber 9/12 Strategy Challenge in which students around the world compete in offering recommendations for how to tackle a fictional cyber crisis.

> "We invested less in [communications and translation infrastructure] to begin with. So that was not the predominant focus of [our strategy]. It was good for connective tissue and benefitted the other pillars of the strategy."
>
> – HEWLETT STAFF

Initiative staff wonder how much more impact could have been possible with additional dedicated funding. Still, despite drawing the smallest Initiative investment (in dollar terms) of the Initiative's three revised strategies, **interviewees praised the effectiveness of Hewlett's contributions to the cyber field's translation and communications infrastructure for its effectiveness**.

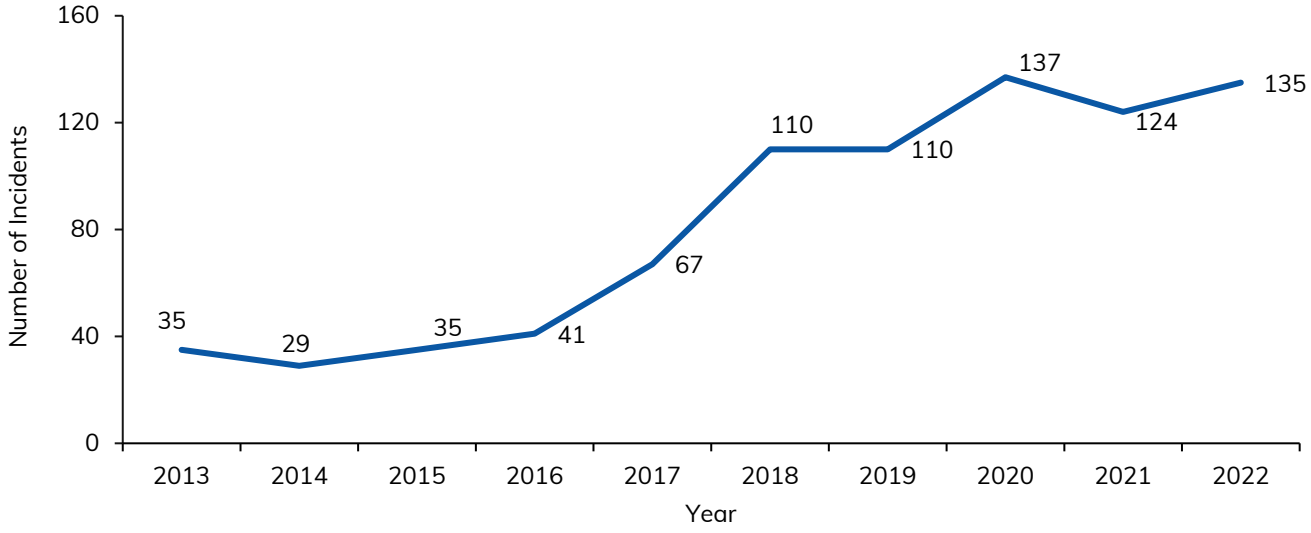
The cyber field has generally gained attention and grown during the Initiative's lifespan. A series of studies commissioned by Hewlett and conducted by Professor Sean Aday of George Washington University analyzed US mainstream media platforms in both print (e.g., New York Times, Washington Post) and television (e.g., CNN, Fox News), and found a steady **increase in coverage of cyber issues** starting in 2015, with coverage being especially high during the 2016 US presidential election due to possible Russian hacking, disinformation and interference, and Hillary Clinton's use of a private email server during her time as US Secretary of State.[34] Coverage peaked in 2019 and dropped off significantly in 2020, likely due to many other newsworthy stories that year including the COVID-19 pandemic, the murder of George Floyd and the subsequent protests and activism that followed, ever-increasing climate disasters, and another presidential election.[35]

The Cyber field has also experienced an increased number of annual incidents requiring greater attention since the Initiative began. The Center for Strategic and International Studies (CSIS) keeps a list of significant cyber incidents since 2006 that were focused on state actions, espionage, and cyber-attacks with losses of over a million dollars.[36] **Exhibit 4** shows the number of attacks noted in the document for each year.

EXHIBIT 4

Number of Notable Cyber Incidents by Year

Source: Center for Strategic International Studies[37]



Aday also found a gradual shift in the backgrounds of those most frequently interviewed and quoted in news stories, as industry and government speakers in the Initiative's early years gave way to expert sources and advocates in later years.[38] This may be due to increased scrutiny of tech companies, as well as the increase in substantive reporting on cyber issues.

Grantees and other interviewees observe **overall improvements in communication and understanding of cyber policy**. A higher volume of accurate, accessible, and understandable information is available to individuals without deep background or expertise in the subject matter. **Journalists and reporters have improved their understanding of and increased their reporting about cyber issues** due to training and professional development opportunities like those supported by the Initiative (e.g., the Verify conferences).

Interviewees' assessment of whether and to what degree these overall improvements in communication have led to increased understanding of cyber among policymakers and the public is mixed. **Communications advances have doubtless helped address what has been described as both a need and an appetite within the government for expertise on cyber policy issues.** One field expert described the Initiative's most significant impact as teaching policymakers about cyber and cyber basics. News coverage has evolved from emphasizing surface-level "hack of the week" stories to stories exploring deeper implications of cyber developments that could be of use to policymakers, like those about the 2016 election disinformation campaigns.

> "[There are] certainly more reporters now who have an understanding of the field and can report it accurately. I still think there are far too few."
>
> – GRANTEE

> "The number of people who can speak both the technical language and the policy business language is really small, unfortunately. I came at this from the policy side, so I had to teach myself a lot of the technical side … [It's] still a challenge, [but] it's definitely better than it was."
>
> – FIELD EXPERT

On the other hand, the uptake, awareness, and interest in cyber issues by the general public do not come close to matching the proliferation of urgent and critical cyber issues facing society. While cyber is no longer a "niche technical subject," in the words of one grantee, gaps and challenges remain that may stem from challenges to the credibility that research institutions face from a politically polarized public, digital literacy gaps, limits in the extent to which information is translated into multiple languages, lack of interest in complex technical and abstract issues, and the effort needed to authenticate information in an environment of noise and disinformation.

Participants in our evaluation concur that **there are still relatively few people who can communicate well about cyber issues**—a problem further exacerbated by the speed at which technology improves (i.e., by the time research and reporting has been published on an issue, rapid changes in technology make the reporting obsolete quickly). Grantees agree journalists are well-positioned to serve as additional conduits of information to the general public. To do this effectively, they need ongoing training to help journalists understand the field's technical aspects and ongoing network expansion to keep them connected to expert sources. While the floor of cyber awareness and knowledge has been raised, some interviewees still wonder if the extent of the public's interest in cyber issues is lower than is reasonable to expect.

> "There are unrealistic expectations about how much the general public cares about cyber."
>
> – CONSULTANT

SPOTLIGHT ON EDUCATING JOURNALISTS TO INFORM PUBLIC OPINION

The Global Investigative Journalism Network (**GIJN**) is an "international association of nonprofit organizations that support, promote, and produce investigative journalism"* that received a three-year, $300,000 Initiative grant in June 2022 for their Cyber-Investigative Journalism Project to train a "global cadre of journalists in advanced cyber-investigative techniques and to integrate them into GIJN's networks of investigative reporters around the world."**

The Initiative's decision to make this grant was spurred by GIJN's 2021 *Reporter's Guide to Investigating Organized Crime* which Andrea Arzaba (GIJN Spanish Editor and Digital Threats Project Director) developed, and which included a chapter on cybercrime. According to Arzaba, the cybercrime chapter took longer than anticipated to complete due to the dearth of knowledge about the topic among investigative journalists. This prompted GIJN to look for ways to strengthen the cyber journalism field. Despite consistent waves of cybercrime, disinformation, digital surveillance, hacking, and harassment, only a handful of journalists had the expertise necessary to conduct and report on cyber investigations effectively. Further, journalists were and are targets of cybercrimes themselves.***

GIJN spent the first months of the Initiative grant gathering a global team of trainers including renowned experts in the fields of disinformation, malware, trolling, and spyware. As GIJN's vision includes disseminating an understanding of cyber that goes beyond male-centric, US-centric approaches, ensuring a truly diverse and global course took some time. Arzaba notes, "We really wanted the program to be global, not only people from the Global North … we're very happy that we have trainers and participants from all over the world."

In May 2023, GIJN inaugurated the first cohort of 23 journalists who came from more than 20 countries across Europe, the Middle East, the Americas, Asia, and Africa. Fellows were selected from a pool of over 300 applicants.† There will be a second cohort in November 2023 and two more cohorts are planned for 2024. The course teaches participants how to investigate the digital environment to understand and expose attacks and manipulation, and how to develop a story pitch. It includes office hours with experts and access to a global network of investigative journalists reporting on digital threats.

For GIJN, it's important to reach people from countries where it is difficult to conduct investigative journalism freely; this requires materials in multiple languages. As a companion to the course, GIJN is developing an English-language guide with the tools and techniques introduced in the training course, with plans to translate the guide into the languages GIJN operates in, including Arabic, French, German, Russian, and Spanish. The full manual, *Reporter's Guide to Investigating Digital Threats,* will be released at the Global Investigative Journalism Conference in Sweden in 2023. *Guide* excerpts have already been viewed over 5,000 times from 97 countries on GIJN's website.

GIJN also envisions a scenario where Fellows may be motivated to develop a similar course in their home language to reach more journalists. "[Cyber] issues are not geographically locked in; they're worldwide. We think it's important to train everywhere—educate and broaden the conversation everywhere, not just in a specific geographic region," says GIJN Development Director Karen Martin.

The Initiative grantee community also provided indirect value to GIJN through its networking opportunities. Martin said a GIJN staff member found attending the Initiative's annual grantee convening beneficial; there, they were able to make new connections while raising awareness of the challenges and importance of cyber-journalism.

According to Martin, GIJN is already hard at work expanding its impact on the cyber-journalism field: "We are in the process of trying to find additional funding… so that we can make a really powerful impact, with large numbers of journalists who go out there and have this knowledge. And it's been a challenge to find that niche of funders who are willing to combine cyber with the journalism aspect of it." But Martin is optimistic thanks to Hewlett's strategic support: GIJN believes it has a model program that can now be easily scaled in both size and reach.

–

* Global Investigative Journalism Network (n.d.). https://gijn.org/

** William and Flora Hewlett Foundation (2022, June 14). Grant to the Global Investigative Journalism Network: For The Cyber-Investigative Journalism Project. https://hewlett.org/grants/global-investigative-journalism-network-for-the-cyber-investigative-journalism-project/

*** The Pegasus Project is a prominent example, targeting more than 200 journalists globally. https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

† GIJN Staff (2023, May 23). 23 Journalists Selected for GIJN's Inaugural Digital Threats Training Course. https://gijn.org/2023/05/15/gijn-launches-inaugural-cyber-digital-threats-training-course/

Diversity, Equity, & Inclusion

Early on, the Cyber Initiative team was attentive to diversity in terms of gender, geographic location, and political viewpoint. Prior to 2021, Hewlett's DEI engagements within the Cyber Initiative had been emergent, such as providing OE grants and funding to support specific DEI-focused projects[39] such as the 2017 grant to the Brookings Institute to create a searchable website compiling the names of women in technology policy (a list that originally appeared on Lawfare's website)[40] or grants to New America to diversify expert voices on digital security policy at the Organisation for Economic Co-operation and Development (**OECD**).

While DEI has been a formal guiding principle at Hewlett since 2018,[41] the confluence of events in 2020 referenced above that increased public awareness of racial inequities and their widespread, damaging effects led the Foundation, like many other philanthropic organizations in the US, to further reflect on its existing work and commit to greater integration of efforts to address the US legacy of racism. In 2020, Hewlett launched a racial justice initiative,[42] created and hired a new Chief of Equity and Culture,[43] and intentionally foregrounded other racial justice and DEI efforts. Foundation staff also began exploring "grants to other institutions serving racially diverse student communities."[44] The commissioning of a 2021 evaluation of the Initiative's talent pipeline strategy also followed Hewlett's emphasis on racial justice. One of the goals of that external evaluation was to determine the extent to which university partners were already serving—or failing to serve—communities of color.[45]

These findings, paired with data trends from Hewlett grantee demographic reports and a Hewlett-funded MITRE report on diversity in the cyber workforce, contributed to two key DEI-focused efforts within the Cyber Initiative in 2022: [46, 47]

1. The Initiative brought on a DEI consultant to work alongside select grantees interested in deeper (especially racial) DEI engagement. While the engagement was intended to follow a uniform cohort approach, grantee uptake varied, leading the consultant to engage more deeply with staff at organizations able to make the time and supporting grantees as they opened important DEI-related conversations with their colleagues. Decreasing grantee participation over time highlighted limitations of the Initiative's consultant-based approach: (1) insufficient grantee organizational leadership interest; (2) limited time and resources to dedicate meaningfully to DEI efforts; and (3) some disagreement amongst grantees as to the relevance of DEI concerns to their work. The first is especially difficult for grantees who are part of a small program within a larger institution where the larger entity is insufficiently supportive of the work.

2. The second was the decision to grant $21 million to the four MSIs mentioned previously: TMCC, FIU, Florida A&M, and Spelman College. Each university's award followed a grant structure similar to the Initiative's initial anchor investments in MIT, Stanford, and UC Berkeley.

Additionally, the Initiative continued to support other DEI efforts more intentionally, including a grant to New America for their #SharetheMicInCyber Fellowship and grants to a new cohort of organizations (Women in Cybersecurity, Govern for America, and Cyber Collective) whose work prioritizes underrepresented communities:

- Govern For America (**GFA**) places broadband and digital fellows from diverse backgrounds into state and local governments in the United States.
- Women in Cybersecurity (**WiCyS**) hosts programs and conferences to recruit, retain, and advance women in cybersecurity.
- Cyber Collective educates and empowers digital natives to think critically about their relationship with technology.

SUPPORTING A DIVERSE CYBER WORKFORCE BY FUNDING MINORITY-SERVING INSTITUTIONS

The following four minority-serving institutions (**MSIs**) received multiyear, multimillion-dollar grants in the closing months of the Cyber Initiative. All four are positioned at critical intersections of increasing the diversity of voices and perspectives in the cyber field.

- **Florida A&M University** will create the **Cyber Policy Institute** to address policy challenges and opportunities by integrating science-based and market-oriented domains of knowledge within the university to help students develop expertise in cyber policy and, ultimately, earn a master's degree in cyber policy.
- **Florida International University** will build on its existing **Cybersecurity@FIU** initiative by expanding its existing teaching and research capacity and supporting the recruitment of students pursuing careers in cybersecurity policy, including the launch of a Cyber Policy master's program.
- **Spelman College** aims to increase the number of Black women in the cyber field through the creation of an undergraduate interdisciplinary minor in cyber policy, an annual speaker series on cyber issues, and the development of a pathway program for Spelman students to complete the Master of Science in cyber policy at a partner school.
- **Turtle Mountain Community College** (**TMCC**) will build on its existing associate degree program in cybersecurity by developing a Bachelor of Applied Science (**BAS**) degree in Cyber Law & Policy to launch in Fall 2024 and prepare Native students for positions in government, industry, and research, as well as provide the foundation necessary for success in graduate programs.

Each of these grants aims to build new or strengthen existing bridges to allow underrepresented groups with unique perspectives a path into the cyber policy field. For example, with Hewlett's support, TMCC is creating the first tribal-focused cyber degree program. For Chad Davis, IT Director at TMCC, the increased emphasis on cyber is about "being able to do the things that we want to do in our tribal government, having access to the information … and being able to have control of our own data and security of that data and not rely on other federal and state governments to hold our data." The program has dual goals of building a pool of Native cyber professionals who will receive Native training in cyber policy and can work within tribal governments on cyber issues, as well as advocate for tribal sovereignty within state and federal policy conversations. Elsewhere, Cybersecurity@FIU Director of Education and Training, Randy Pestana, noted intentional foci on getting more women involved at FIU and addressing a lack of Hispanic thought leaders in the cyber community.

Lastly, while strides have been made in Black representation in cyber leadership positions (e.g., two Black women serve in the Biden administration as Acting National Cyber Director and Deputy National Cyber Director,), Florida A&M and Spelman College will play a key role in further reducing the representation gaps. Dr. Raquel Hill, Professor and Chair of Spelman's Computer and Information Sciences Department that will develop an interdisciplinary cyber program in collaboration with its Political Science Department, emphasized the importance of having "focused and concentrated [cyber policy] training" in order for MSIs to have an impact and "become leaders" in the space.

Underpinning each MSI's work is a sense of urgency deriving from the later timing of their Cyber Initiative awards. Because Hewlett made their grants to these four institutions as the Cyber Initiative winds down, the MSIs will not receive the same long-term active support and guidance the Foundation provided to Stanford, MIT, and UC Berkeley. Nonetheless, the awards will deliver increases in the number of degree programs offered, as well as in the annual student acceptance and enrollment numbers. As Hewlett exits the field, ongoing funding from other grantmakers will be crucial to ensuring racial and ethnic diversity receive the same level of intentional attention the Initiative gave to gender, geographic, and political viewpoints in its efforts to diversify the field of cyber policy.

As Davis shared: "I know that I'm part of a small group of Native Americans in cybersecurity, but I'm determined to make a difference. I believe it is important to raise awareness of the importance of cybersecurity education and to promote the work of tribal colleges like Turtle Mountain Community College which are working diligently to train the next generation of cybersecurity warriors."

Interviews demonstrated that grantees think about diversity expansively and ways they have addressed several aspects of DEI through their work. Dimensions of diversity noted by grantees included class, caste, formal education level, geographic location, age, political ideology, disability and neurodiversity, academic discipline, race, and gender. Interviewees believed in the promise and potential funding MSIs have for diversifying the talent pipeline but lamented how late in the Initiative grants were awarded, as MSIs could have benefited from the same networking and collaborative gains enjoyed by long-term grantees if they were awarded grants sooner.

The State of the Field in 2023

As compared to the start of the Initiative, the cyber field in which grantees operate is much stronger and more well-connected, with greater awareness about cyber threats to critical infrastructure. However, ongoing support is critical to maintain momentum in the field, especially as technology advances at an accelerated pace. Grantees have, for the most part, accepted the sunsetting of the Cyber Initiative. Given how significant the Foundation's portion of their funding has been however, some thought Hewlett should have engaged other funders more proactively and earlier on in the Initiative despite recognizing that it is tough to convince funders to take on new areas of interest.[48] While not anticipating other funders will take a similar cyber policy field-building approach, Foundation staff hope others will support specific cyber topics or projects that overlap with or relate to areas they already fund or have an interest in funding.

While academic institutions usually have built-in funding streams, think tanks and other civil society organizations cannot rely on the same stability, leaving them at a funding disadvantage. One academic grantee added that despite having built-in funding streams, these streams are highly competitive to access and typically permit only project-related spending rather than covering core costs. They can neither replicate nor replace Hewlett's flexible funding. Some grantees worried the Foundation's exit will mean they need to rely on government and industry funding, which they fear may put the legitimacy of their funded work at risk, given the vested interests of these sources. Even if grantees can generate interest from additional donors, Hewlett's departure will leave the field without a supporter uniquely focused on building a multidisciplinary field, rather than focusing on specific issues, as many funders do. In addition to sustainability efforts implemented midway through the Initiative (see Winding Down of the Initiative, above), Hewlett has retained a fundraising consultancy for several years to build the long-term fundraising capacity of grantees. In response to anxieties about a post-Hewlett funding shortage, the Initiative also commissioned Camber Collective to conduct a funder landscape scan. This scan provides the Foundation with insights into other funders' cyber-related portfolios and offers Initiative grantees the same information, leaving them with potential funding prospects as Hewlett exits the field.[49]

LESSONS & REFLECTIONS

Overall, grantees expressed immense gratitude and appreciation for Hewlett's overarching grantmaking approach, and **many credited the Cyber Initiative with significantly advancing their work.**

> "To the extent we've done anything, that was all because of Hewlett. We wouldn't have started in the field, number one. Number two, they gave us enough resources that I could hire people, often [bringing] them into the field and [telling] them they can learn how the outside world works without the pressure of having to go out and immediately raise money for their work."
>
> – GRANTEE

Hewlett staff engaged with grantees in ways that created an environment of trust and partnership. Many interviewees (grantees, consultants, and experts alike) emphasized their deep appreciation for Foundation staff and the ways staff engaged with them. Grantees noted feeling a sense of independence and viewed Foundation staff as trusting supporters. The Hewlett team did not mandate that grantees' work reflect any particular viewpoint, nor did they direct grantees in what to write or ask to review reports in advance of publication. Additionally, the Initiative's minimal grant requirements gave grantees the ability to do their work without being tied to specific deliverables or spending excessive time completing reporting tasks.

Grantees also highly praised the knowledge, skill, and overall quality of the Initiative staff. They described Hewlett staff as thought partners who engaged in conversations that led to new programs, adjustments in their strategies, potential collaborations across the field, and introductions to other funders. Interviewees commended the Foundation staff's ability to engage them with humility and expertise. Many admired how well Cyber Initiative leadership understood the grantees and how able and willing they were to make connections on their behalf.

While some grantees commented on the need for greater capacity on Hewlett's side (i.e., more dedicated staff for the Initiative), small teams are an intentional tactic the Foundation uses to prevent micromanagement and support the low-burden engagements grantees highly regard.[50]

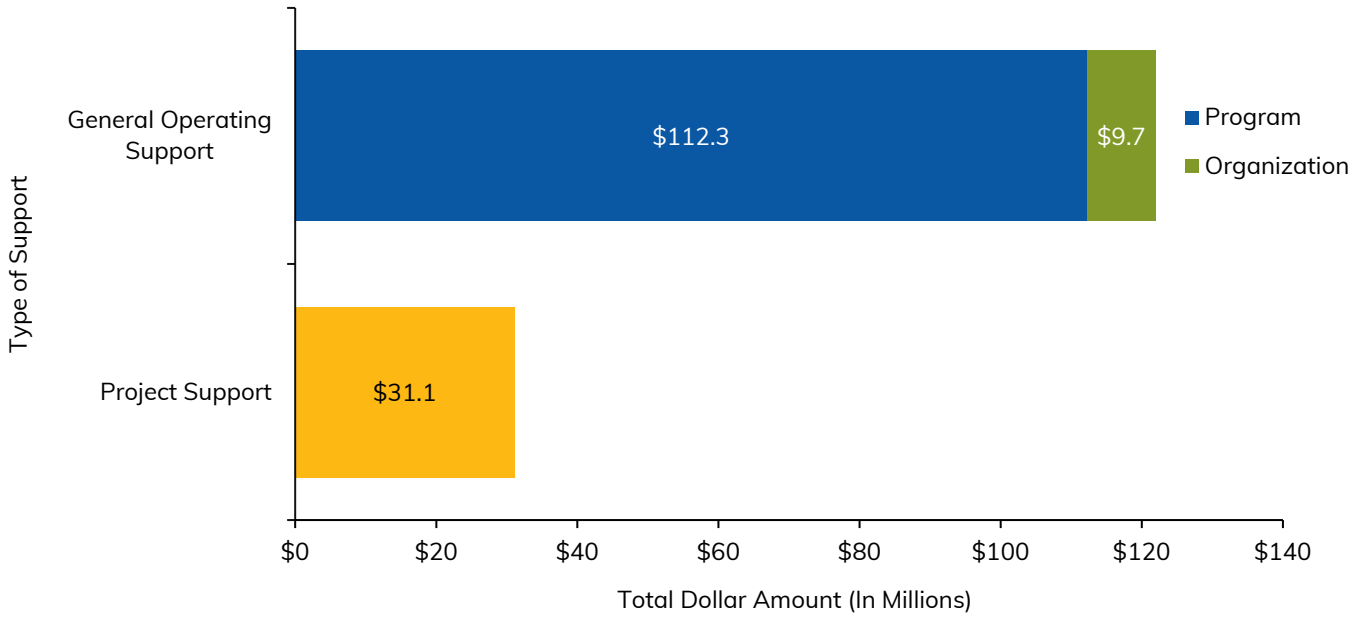
> "Hewlett never asked to look at our reports before we sent them out; as a result, we never felt that we had somebody looking over our shoulder. That degree of trust in what we were doing was very meaningful. I believe it helped make our analysis more impactful. We could honestly say we were nonpartisan. It's important to us that we don't have an ideological bent—conservative, liberal, etc. We were and still are focused on data-driven analysis, and Hewlett allowed that to happen."
>
> – GRANTEE

> "There was no micromanagement in the grant, which is huge because so many [sources of funding], whether they are academic or [not], require reporting all the way along, sometimes very detailed, and justifying everything. So, you feel like you're not trusted for doing the right thing. And here, I had the feeling that they really took time to decide to fund us and then they fully trusted us, and they were here to help us. And we had time for research because the grant was over three years as opposed to grants that require renewing every year and reapplying every year and that was really precious. So, I really love this model. I think it's the best model."
>
> – GRANTEE

The Foundation's approach to grantmaking gave grantees the freedom to do what they do best. Grantees also spoke highly of the types and amount of funding provided through the Initiative. Most Initiative dollars were flexible across programs or organizations, with a smaller amount dedicated to specific projects (**Exhibit 5**). Like many nonprofit leaders, grantees heartily endorsed the benefits of receiving multi-year general program support, which allowed them to remain nimble and do what was most relevant and needed for their projects and programs without having to take time away from the work to chase additional funding. (General program support—akin to general operating support—was necessary for programs within larger entities such as universities; funds went directly to the Initiative-funded project or program rather than being shared with the parent institutions.) Grantees also noted Hewlett grant amounts provided sufficient resources and time to develop substantial work they could use to demonstrate their value to other funders.

EXHIBIT 5

Total Granted Dollar Amount (in Millions) by Type of Support (As of August 2023)



While this style of grantmaking and grantee management (e.g., multi-year, flexible, requiring minimal reporting, trust-based) is now standard practice by some foundations, Cyber Initiative grantees described the experience as distinctive and key to the Initiative's successes.

DEI objectives and efforts require thoughtful integration into the DNA of an initiative from the start. When asked to reflect on how the Initiative panned out, grantees most notably called attention to limitations in how the Initiative integrated DEI approaches (or did not) into its fabric. While diversity was a cross-cutting theme throughout the Initiative, focusing largely on geography, political ideology, and gender from the outset, and expanding to include race in later years, grantees nevertheless noted it as an area for improvement. For example, thought leadership was still relatively homogeneous and limited; this was reflected in Cyber Initiative convenings, which consisted mostly of attendees with Global North perspectives. Grantees also noted they had limited opportunities to discuss more holistic cyber DEI practices that went beyond just "diversity hires."

> "[A panel said] 'Just hire more Black people and hire more Hispanic people and hire more women' and I agree with all of that. But I would say, how do we hire and integrate more women? How do we hire and integrate more Black [people]? How do we hire and integrate more Hispanics? So that would be a better approach in my estimation as opposed to just saying, 'Hey, we're just hiring to hire.' ... It's a 'No, we're intentional about this.'"
>
> – GRANTEE

Another interviewee noted many ways in which one can think about diversity, "in terms of things like gender and ethnicity, but also in terms of big schools, small schools, R1 [versus] non-R1 universities, geographic diversity, everything on the coast versus [non-coastal regions]. I don't think the way it was done helped in that regard and was a missed opportunity."

Lastly, another limitation that may have impacted DEI efforts was the fact that some grantees (namely universities and some international organizations) had legal constraints making explicit attention to gender and racial/ethnic DEI more difficult. This will likely continue to pose a challenge in future efforts with grantees in those contexts.

Before there was any sense of a "field," it made sense for Hewlett to take the lead in building something that could attract future funders. In 2014, Hewlett observed that most other funders would have found entering the cyber policy space too challenging to be attractive. To the degree other funders considered it, they were likely to have struggled to find candidates with the right kinds of connections and expertise to direct a grantmaking program. Further, few foundations are willing to take financial risks on portfolios or grantees whose impacts are uncertain and difficult to measure. This would seem to support Hewlett's approach of initially entering the cyber policy space as a near-sole funder.

However, it may be worth exploring whether more collaborative funding can have more than an additive effect and better set up grantees for post-funding sustainability. Some interviewees argued Hewlett's engagement of other funders should have happened even earlier, and that funders would have been more likely to participate if they had been approached as partners early in the work, as opposed to being positioned only as following in Hewlett's footsteps once they depart the field.[51] The interviewees surmised that the Cyber Initiative's large early investments may have disincentivized other funders from engaging because they might have perceived their own entry into the space to be unnecessary, assumed the field required multi-million-dollar grants to have any notable impact, or both.

Several interviewees commented on Hewlett's strategy for engaging other funders to support cyber policy, noting that the Initiative could have benefited from other funders earlier on and perhaps in partnership with one another rather than as after-the-fact individual invitees. However, perspectives on the **pros and cons of how and when to engage other funders** varied across those involved with the Initiative. The table below lists the most prominent pros and cons that surfaced in Informing Change's conversations with grantees about this topic.

PROS: Funding partnerships can…	**CONS:** Depending on how they are structured, funding partnerships may, or do, require…
• Create a shared sense of responsibility for a particular field. By spreading this sense across multiple funders, it can, in turn, result in greater awareness of an issue area. • Create opportunities for larger amounts of funding and potentially greater impact. • Increase exposure for grantees to multiple funders thereby increasing access to ongoing and other resources and opportunities.	• Slower decision-making. • Grantees to meet the demands of multiple funders. • Greater alignment, communication, and coordination across funders, compounded by differing governing boards' often inflexible obligations that can result in undue burdens on grantees. • A single point of contact across funders which can limit relationship building and exposure for grantees' current and future efforts.

More proactive, concrete communication to grantees about how much and what forms of capacity-building support were feasible from each consultant may have helped increase the uptake and utility of Hewlett's technical assistance offerings. Hewlett contracted with two communications firms and a fundraising consultant to offer grantees some capacity-building support in each area. Some grantees found this support valuable; others did not receive the kind of help they were hoping for. Consultants, for their part, were disappointed at the limited grantee uptake of their offerings and wished they had had more opportunities to showcase what they could offer so that grantees knew what was available to them.[52] Similarly, Hewlett staff expressed disappointment that these strategies were not as successful as they'd hoped.

There is much room to support, and a continued need for, multidisciplinary research exchanges. Cyber Initiative grantees widely agree such exchange is crucial for urgent cyber policy problems in rapidly changing contexts. **Designing high-quality convenings are a good way to do this**, as are funding conference travel and helping scholars and other experts connect and network with one another.

While the Cyber Initiative did not set out to increase the number of tenured scholars in cyber policy, some interviewees clearly perceive the small number of tenured faculty with multidisciplinary cyber training as a disappointing indicator for the field. However, this goal is difficult (if not impossible) for philanthropies to achieve as a talent-pipeline outcome, for many reasons—time-to-tenure, limited availability of positions, and disciplinary traditions, to name a few.[53] Encouraging scholars already on the tenure track to prioritize multidisciplinary knowledge acquisition and research may not be the best use of Foundation dollars, if only because the institutional barriers to achieving tenure with these qualifications are still very high and will likely be slow to change. Foundation staff note that tenured professors do run select Initiative-funded centers or programs, but the Initiative's goal was to focus on promoting multidisciplinarity, program formality and maturity, and staying power. This left open a door for institutions to determine which approaches best fit their and their students' needs. For example, at least one academic grantee used grant funding to establish an endowed chair position to meet its goals.

Finally, grantees observe that **the division between tech and policy experts persists,** despite some real success in narrowing it. Ongoing and intentional investments to continue reducing disciplinary and sector fragmentation will be essential for continued progress in this area.

CONCLUSION

There have been substantial gains in the development of the stronger cyber field the Foundation set out to seed and catalyze. Regardless of whether they are due to the direct or indirect contributions of the Cyber Initiative, **these gains are a cause for celebration and showcase exciting and necessary areas for future investment.** This evaluation has captured many important questions for the field to grapple with that philanthropy is uniquely positioned to support the field in answering. Philanthropy can fill gaps that neither government, nor industry, nor academia can fill alone.

QUESTIONS STILL FACING THE FIELD

As we spoke to the researchers, experts, and funders of a still-developing cyber field, three recurrent, overarching questions emerged:

1. How can policymakers keep up with technological progress, both in understanding and creating relevant policies? The pace of technology moves far too quickly for policymakers to develop timely and relevant policies and frameworks, and technology is often put to market without even its creators fully understanding the potential vulnerabilities or security ramifications. This keeps policy conversations in a constant cycle of reactively responding to problems rather than proactively seeking to prevent them.

2. What is the ideal relationship between government and industry when it comes to cyber, given that:

- Government is both a regulator of the cyber field and a buyer of goods and services from cyber industries.
- Digital infrastructure is almost entirely owned and operated by private companies, which has implications for information security and the power industry holds in policy debates.

3. How much regulation is ideal—or even possible in the cyber policy field?

- *Domestically*, private tech companies and others in the cybersecurity industry occupy a paradoxical space. On one hand, they have prevented or stalled regulation when it would interfere with their ability to maximize profits. However, they also play a role in keeping government bodies in check by protecting the privacy of consumer data from government surveillance.
- *Globally*, what is the private sector's role in geopolitical struggles and conflicts that play out in the cyber realm? Digital infrastructure, including the servers and platforms that control water, power, healthcare records and machinery, and other critical resources is often vulnerable to manipulation by adversaries and can be crucial in defense. When these platforms are owned and operated by the private sector, how should they cooperate or participate in geopolitical conflicts?*

–

* The private sector contracting with various military bodies both domestically and abroad is not a new phenomenon, but the war in Ukraine has brought cyber-related issues that cross lines between private and military sectors to the forefront and made them stark realities, especially as they can impact the safety and security of civilians and refugees.

Informing Change has learned through this evaluation that **funders need not possess deep technical expertise to enter and engage the cyber space successfully** and that **the need for support is ongoing and urgent**. We've learned that part of what made the Initiative so successful was the humility and openness Hewlett staff brought with them to the experts they consulted and to those they funded, and the effectiveness with which they brought grantees together and connected them to each other. The Initiative's other source of success lay in the Foundation's overall approach to grantmaking: one that minimizes many of the typical

burdens associated with receiving grant funding and allows grantees to do what they do best, permitting enough flexibility for them to adapt to emerging needs.

At a field level, **private industry, government, academia, and the public have a greater awareness of the benefits and threats associated with cyber technology, and there are more and better-informed players in sites of policymaking**; policymakers also have more accessible information at their fingertips. Hewlett learned about the valuable strategy of educating journalists in fields like cyber that affect the world at large but also pose high knowledge barriers. [54] Overall, **communication about cyber and cyber-related issues has grown and improved since the Initiative's start, and there is much more room to grow**: the pool of people who can effectively communicate about cyber issues remains small because of the field's rapidly evolving complexity.

The talent pipeline and research spaces have seen an increase in multidisciplinary academic programs well set up for continuation beyond the Initiative, as well as an increase in capable candidates for US government positions. Yet many opportunities exist to continue investing in a broader set of academic institutions to further diversify and strengthen the field. Think tanks have also contributed through their increased focus on cyber issues and research that has helped inform policymakers. However, it remains unclear whether Initiative-funded think tanks (and other non-academic civil society organizations) have the funding necessary to ensure their longevity after Hewlett departs. **Many think tanks continue to rely heavily on the Foundation and have struggled to diversify their funding** sources in recent years. (Hewlett funding makes up 24% of all current grantee budgets, with 10 current grantees facing the prospect of losing at least 50% of their funding when Hewlett exits.[55]) Those without the stable infrastructure of academic institutional homes that can provide non-grant sources of funding are vulnerable to closure.

There exists greater collaboration and organization across sub-fields within cyber. Hewlett sought to create a field with experts capable of making policy choices informed by multiple perspectives through an emphasis on multidisciplinary education and collaboration. Even as grantees continue to grapple with ethical, technical, and other quandaries in as-yet-uncharted waters, **the Initiative has resulted in substantial progress over the last decade toward the kind of multidisciplinary cyber field that Hewlett envisioned**.

The ongoing nature of the challenges discussed in this report—and more importantly, the dispersed and siloed nature of the experts capable of helping policymakers grapple with them—helped propel the creation of the Cyber Initiative. There is still more work to be done in building a comprehensive field-wide body of policy-relevant knowledge and experience across cyber-related disciplines. Yet **Hewlett leaves behind a richer and more collaborative field of experts** to clearly define the problems in need of solution and to inform policy makers as they seek to identify these solutions. While silos remain, **there is more active information exchange between experts and policymakers as they attempt to chart a path forward through the thickets of cyber threats to privacy and security**. For this, we are fortunate because, as many of our interviewees eloquently stressed, these questions and threats become ever more critical to address.

> "There are really important questions … becoming more real and less hypothetical every day about the role of cyber in armed conflict that will not be funded unless someone takes up the mantle from Hewlett. … Companies themselves are not incentivized to talk about [those things] and without … funding for [the] study of [them], the field will languish at a really important time."
>
> – FIELD EXPERT

Without a doubt, cyber and cyber-related issues will remain urgently relevant and important areas of exploration for the foreseeable future. Given their complexity and the innumerable ways they intersect with a variety of issue areas (e.g., health, education, climate, arts), there are many opportunities for funders to support and have great impact in this ever-evolving field, and we agree with Hewlett that it is vital for them to do so.

ENDNOTES

[1] The Cyber Initiative staff and their documents, as well as research participants in this study, often used the terms multidisciplinar(it)y and interdisciplinar(it)y interchangeably. We have followed suit in this report although multiple scholars have argued against interchangeable usage (e.g., "The common words for multidisciplinary, interdisciplinary and transdisciplinary are additive, interactive, and holistic, respectively. With their own specific meanings, these terms should not be used interchangeably" https://pubmed.ncbi.nlm.nih.gov/17330451/). We have elected to ignore such guidance here because we were usually unable to discern from context which meaning a writer or speaker intended.

[2] Kramer served as the Richard E. Lang Professor of Law and Dean of Stanford Law School from 2004 to 2012.

[3] Grantees point out key differences between cyber policy, cyber, tech(nology), and tech policy (among other distinctions) that are sometimes obscured in Cyber Initiative documents. For more on this, please see the text box "What's in a Name?" on page 15.

[4] Sugarman, E. "Refining Our Cyber Initiative Grantmaking Strategy," *Hewlett Foundation* (blog), March 22, 2016, https://hewlett.org/refining-our-cyber-initiative-grantmaking-strategy/.

[5] The selection of three elite universities (MIT, Stanford, and UC Berkeley) to receive multi-million-dollar grants was also enabled, if not prompted, by an unexpected surplus of funds at the end of 2014. For tax-related reasons, the Foundation needed to grant these dollars within the calendar year and had to make quick decisions about the best way to do so. Recipient schools were permitted, however, to use the funds over the course of 3-5 years.

[6] These three core outcomes were pared down from five original core outcomes as part of a Foundation-wide effort to reduce the number of objectives and implementation markers for each of Hewlett's programs and initiatives. For a timeline of key outcomes and implementation markers, please see **Appendix A**.

[7] 10 grants serve both US and International and are counted in both categories. This exhibit does not include Direct Charitable Activities (DCAs).

[8] Organizational Effectiveness grants supported capacity-building efforts at existing grantee organizations. Typical activities these grants funded included strategic planning, fundraising capacity-building, and organizational development related to staffing, technology, or communications.

[9] The William & Flora Hewlett Foundation. *About Us: Our Programs.* https://hewlett.org/about-us/our-programs/

[10] See **Appendix B** for additional detail, including a summary of all reports commissioned by The Hewlett Foundation for this Initiative and a review of Informing Change's decisions regarding the approach and methods for this summative evaluation.

[11] Prompted by the Hewlett Foundation, Informing Change initially considered framing the evaluation in terms laid out by The James Irvine Foundation & The Bridgespan Group's The Strong Field Framework: A Guide and Toolkit for Funders and Nonprofits Committed to Large-Scale Impact (**SFF**). While our evaluation questions did not use the SFF, our protocol design did in part. Later, however, we and the Hewlett Foundation staff opted not to use this framework due to aspects of the cyber field the tool is not well-suited to assess. For a more detailed discussion, see **Appendix C**. The SFF can be found online at https://irvine-dot-org.s3.amazonaws.com/documents/64/attachments/strongfieldframework.pdf?1412656138Bridgespan/.

[12] The Cybersecurity Act of 2012 was cited by many interviewees as a missed opportunity by the federal government to put into place comprehensive protective cyber policies. The Act was an effort to create a set of minimum mandatory standards that would govern both government and industry in the face of increasing cybersecurity threats. However, it was blocked in Congress through a filibuster, in part due to opposition arguments that the required information-sharing between industry and government would put consumer data at risk and would be burdensome to industry.

[13] For instance: the Cybersecurity and Infrastructure Security Agency within the Department of Homeland Security (established in 2018), the Office of the National Cyber Director within the White House (established in 2021), the Bureau of Cyberspace and Digital Policy within the State Department (established in 2022), the Cybersecurity Unit of the Security Operations Center within the Department of Justice (established 2014), the U.S. Cyber Command within the Department of Defense (established 2010), the Information Operations Center within the CIA, the National Cyber Investigative Joint Task Force within the FBI (established in 2008), and other offices within the GAO, NSA, and others.

[14] For instance: the 2016 US presidential election brought up multiple issues covered by Hewlett's coverage of "cyber": 1) Russian hacker groups hacked and leaked Democratic National Committee emails via WikiLeaks in order to influence election results; 2) Russian operatives also launched disinformation campaigns using social media to influence voters; and, 3) the security of digital voting machines, which were run by private companies with little government oversight, was brought into question.

[15] Aday, S. (2020). Covering Cyber: Media Coverage of Cyber Issues: 2019-2020. Institute for Public Diplomacy and Global Communication, George Washington University. Unpublished internal document.

[16] The UN norms of responsible state behaviour in cyberspace; Council of Europe's AI and Human Rights guidance; NIST cybersecurity framework.

[17] The EU's GDPR became effective in 2018. While California passed the California Consumer Privacy Act (CCPA) in 2018 (effective in 2020), legislation very similar to the GDPR, federal policymakers are still trying to determine which pieces of the GDPR might be incorporated into US regulations.

[18] For a more detailed list of influential cyber events, see the Center for Strategic & International Studies list of Significant Cyber Events Since 2006. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404_Significant_Cyber_Events.pdf?VersionId=3UxjuqXLPluSCUtSXhGM1ZecgewJ4wPI

[19] It is difficult for tenure-track faculty to achieve tenured status in most US colleges and universities if they do not show a record of peer-reviewed publications in their "disciplinary home." Scholars with entirely multi- or interdisciplinary training and publication records often have a very difficult time getting published in traditional disciplinary journals, which makes it especially hard for them to achieve tenure. As a result, untenured faculty are often discouraged from developing cross-disciplinary expertise or publishing across disciplinary boundaries.

[20] Camber Collective. (2018). Hewlett Cyber Initiative: Grantee reporting and survey results. Unpublished internal document.

[21] Camber Collective. (2022). Cyber Initiative 2021 MLE Summary Deck. Unpublished internal document.

[22] Camber Collective. (2016). Evaluation of Network Building: Grants & Beyond-Grant Activities. *The William & Flora Hewlett Foundation.* https://www.hewlett.org/wp-content/uploads/2018/02/Evaluation-of-network-building-Cyber-2018.pdf

[23] Camber Collective. (2023). Cyber Initiative 2022 MLE Summary Deck. Unpublished internal document.

[24] Camber Collective. (2023). *Cyber Initiative 2022 MLE Summary Deck.* Unpublished internal document.

[25] Untenured faculty continue to be hired primarily by traditional disciplinary departments and rewarded for work within that singular discipline. See note 20.

[26] Many Hewlett grantee scholars, however, have created, edited, and/or published in interdisciplinary journals, such as the *Yale Journal of Law and Technology, Journal of Financial Transformation, Journal of National Security Law & Policy*, and others (as reported in the Camber Collective's annual survey).

[27] Camber Collective. (2023). *Cyber Initiative 2022 MLE Summary Deck.* Unpublished internal document.

[28] Private industry continues to play a significant role in diverting academic and think tank researchers from potential policymaking employment by attracting them with offers of much higher salaries and benefit packages. Since many private companies can exert powerful influence on public policy, it may be plausible to argue that Hewlett-funded organizations have still contributed to the pipeline of workers who inform policy at least indirectly via their private employment.

[29] Hewlett Foundation (2022). Request for Proposals: Cyber Initiative Summative Evaluation.

[30] Hewlett Foundation (2022). Request for Proposals: Cyber Initiative Summative Evaluation.

[31] Grantees reported 351 instances of engaging in informal consultation and 52 instances of congressional testimony from 2016 to 2022 (combined data from the Camber Collective's annual survey for non-academic civil society grantees).

[32] Methods for taking account of such "off the record" consultation and information exchange do exist in the field of policy advocacy, but their use was either inappropriate due to prior data limitations or simply beyond the scope of this evaluation.

[33] Wickline, H. (2022). Three Takeaways from Verify 2022. https://hewlett.org/three-takeaways-from-verify-2022/

[34] Aday, S. (2018). Covering Cyber: Media Coverage of Cyber Issues Since 2014. Institute for Public Diplomacy and Global Communication, George Washington University. Unpublished internal document.

[35] Aday, S. (2020). Covering Cyber: Media Coverage of Cyber Issues: 2019-2020. Institute for Public Diplomacy and Global Communication, George Washington University. Unpublished internal document.

[36] Center for Strategic & International Studies (CSIS). (2023). Significant Cyber Events Since 2006. https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-04/230404_Significant_Cyber_Events.pdf

[37] Center for Strategic & International Studies (CSIS). (2023).

[38] Aday, S. (2018 and 2020).

[39] Community Wealth Partners (2019, September). Hewlett Foundation OE-DEI Grants Final Report. https://hewlett.org/wp-content/uploads/2019/12/Hewlett-Foundation-OE-DEI-Grants-Report.pdf

[40] Wickline, H. (2018, May). Lifting up new voices in tech policy: Four questions for Susan Hennessey. https://hewlett.org/lifting-up-new-voices-in-tech-policy-four-questions-for-susan-hennessey/

[41] Kramer, L. (2018, January 16). Committing to diversity, equity and inclusion. The William & Flora Hewlett Foundation. https://hewlett.org/committing-diversity-equity-inclusion/

[42] Kramer, L. (2020, July 16). New steps to address systemic racism. The William & Flora Hewlett Foundation. https://hewlett.org/new-steps-to-address-systemic-racism/

[43] The William & Flora Hewlett Foundation (2021, March 5). Hewlett Foundation names Charmaine Jackson Mercer as first-ever Chief of Equity and Culture. https://hewlett.org/newsroom/hewlett-foundation-names-charmaine-jackson-mercer-as-first-ever-chief-of-equity-and-culture/

[44] Hewlett Foundation. (2020, October). Program Budget Memo: Cyber Initiative. Unpublished internal document.

[45] Nelson, J. & McGuinness, C. (2021). The Hewlett Foundation's Cyber Talent Pipeline: An evaluation based on Equitable Evaluation Framework™ principles. The William and Flora Hewlett Foundation. https://hewlett.org/wp-content/uploads/2021/07/Final-Cyber-Evaluation-2021.pdf

[46] Center for Effective Philanthropy. (2021). The William & Flora Hewlett Foundation 2019 Demographics Report – Cyber. And Center for Effective Philanthropy. (2022). The William & Flora Hewlett Foundation 2021 Demographics Report – Cyber. Both reports show significantly less gender and racial/ethnic diversity among Cyber grantees than the larger Hewlett grantee pool.

[47] Lachlow, I. (2022). Diversity in the Cyber Workforce: Addressing the Data Gap. MITRE. https://www.mitre.org/news-insights/publication/diversity-cyber-workforce-addressing-data-gap (compiling research into why diverse teams matter in the workplace).

[48] Camber Collective. (2023). Cyber Initiative 2022 MLE Summary Deck. Unpublished internal document.

[49] *Camber Collective. (2023). Cyber Funding Landscape Summary. Unpublished report.*

[50] Stid, D. (2022). *The Hewlett Foundation as a formative institution.* https://hewlett.org/the-hewlett-foundation-as-a-formative-institution/

[51] While recognizing the 20:20 hindsight effect, it is conceivable that had Hewlett brought together funders to join it in establishing a field from the beginning—or even much earlier on—this might have had the same risk-reducing effects for those funders as did Hewlett's own large independent investments. Perhaps the partner-funders could have staggered their exits, or even decided to adopt permanent funding lines.

[52] It was notable to us that we did *not* hear a refrain that is by now common among nonprofits: that their infrastructure is simply too lean to take advantage of capacity-building (or organizational effectiveness) grants.

[53] Tenure clocks at most universities are approximately 7 years from date of first Assistant Professorship, though they can be longer for interdisciplinary programs. Students in Cyber Initiative-funded programs who go on to seek academic tenure may yet achieve it. It is simply too soon to say. At the time of this evaluation, most graduates had not entered Hewlett-funded pipelines long enough ago to have acquired tenure track jobs, still less to have reached the point where they can stand for tenure. However, the seeding of interdisciplinary departments (as opposed to certificates and programs) may eventually lead to unique departmental norms that approximate—or even speed up—the time-to-tenure period.

[54] This is a strategy that others have used to good effect. For just one example, the Stanley Center for Peace and Security (formerly The Stanley Foundation) has since 1967 had the practice of connecting journalists with experts who can help them understand complex and overwhelming issues.

[55] Camber Collective. (2023). *Cyber Initiative 2022 MLE Summary Deck.* Unpublished internal document.

Appendices

Appendix A: Outcomes & Implementation Markers Over Time

EXHIBIT A1
Outcomes over Time

HEWLETT CYBER INITIATIVE STATED GOALS									
2014	**2015**	**2016**	**2017**	**2018**	**2019**	**2020**	**2021**	**2022**	**2023**
(1) Begin to develop a network of cybersecurity experts.	**(1)** Build the capacity of individual policymakers to make informed decisions. **[Revised in 2016]** Build the capacity of decision-makers and influencers.		**(1) Goal—Talent Pipeline**: Create a talent pipeline to produce experts with the necessary mix of technical and non-technical skills and knowledge to staff these and other institutions, including government and industry.						
(2) Help individuals and institutions develop comprehensive analyses of cybersecurity problems and solutions.	**(2)** Build a robust network of experts (government, industry, academia, think tanks) that builds trust and collaboration. **(3)** Build the capacity of civil society organizations.		**(2) Goal—Core Institutions**: Build a set of core institutions with sufficient depth of expertise to deliver solutions that take competing values and trade-offs to pressing cyber-policy challenges seriously.						
(3) Attract new funders and additional funds.	**(4)** Catalyze additional funding from philanthropic, government, and private sector sources.								
(4) Fill critical research gaps.	**(5)** Support policy-relevant new research, writing, and thought partnership.		**(3) Goal—Translation/Communication Infrastructure**: Support the development of infrastructure to translate and disseminate the work of these institutions into forms that can be understood and used by decision-makers and the public.						

EXHIBIT A2
Timeline of Implementation Maker Changes

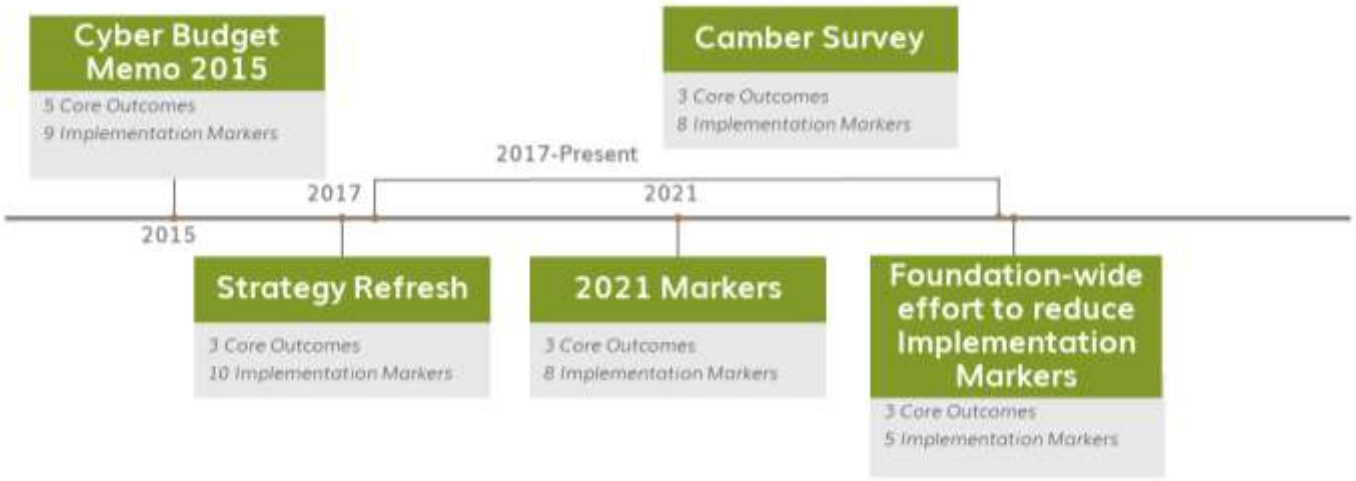


EXHIBIT A3
Table of Implementation Markers Since 2017 Strategy Refresh

CYBER: CORE CIVIL SOCIETY INSTITUTIONS			
2017 MARKERS	CAMBER MARKER	2021 MARKER	2022 MARKER
Ideological & staff diversity: Our portfolio is increasingly ideologically diverse, and within each org the staff is increasingly interdisciplinary, possessing the intellectual resources to bridge technical and policy domains.	**Staff quality and breadth of backgrounds**	**Diverse and growing teams**: Evidence of teams becoming more interdisciplinary and integrating with one another.	X
Response to cyber events: Grantees are amongst the leading responders proposing viable solutions to 3 or more of the "top 5" cyber debates/events each year.	**Impactful response to cyber debates**	**Working with public and private sector leaders to respond to major cyber events and challenges**: % of top 5 cyber events/crises in given year grantees responded to and influenced outcome.	Same text as 2021
Talent pipeline: Outcome 1 grantees are also contributing to talent pipeline development (e.g., by directly employing or creating fellowship opportunities for up and coming cyber experts).	Policy relevant research (Camber's own addition)		

CYBER: TALENT PIPELINE			
2017 MARKERS	CAMBER MARKER	2021 MARKER	2022 MARKER
Diversified funding: Grantees are on path to financial sustainability evidenced by Hewlett making up a smaller yearly % of budget and hiring of non-policy staff.		**Sustainable financing**: Current % of grantee's overall budget funded by Hewlett, as well as efforts to diversify/increase funding to the field overall.	X
Student outcomes: Majority of "graduating" students are entering the field of cyber policy, and heading to positions in a diversity of industry types (e.g., industry, govt, civil society, post doc, etc.).	**Student outcomes**	**Student demand and outcomes:** # of those enrolled or applying as well as % of graduating class headed to industry, govt, civil society, post doc and # of positions they secure.	Same text as 2021
Diverse & accomplished staff: Grantees' faculties, staff, fellows, etc. are increasingly interdisciplinary and new/open positions are being filled quickly.	**Field diversity**	**Improved racial and gender diversity** amongst programs' student bodies.	X
Response to cyber events: Grantees are amongst the leading responders proposing viable solutions to 3 or more of the "top 5" cyber debates/events each year.			

CYBER: TRANSLATION/COMMUNICATION			
2017 MARKERS	CAMBER MARKER	2021 MARKER	2022 MARKER
Increased media coverage: Mainstream media's coverage of cyber increases and is increasingly nuanced. Additionally, our grantees are more frequently cited as experts and/or directly publishing highly-viewed and/or otherwise clearly influential article, papers, etc.	**Increased media coverage**	**Media coverage of cyber policy**: increase in stories on cyber policy and # of civil society experts cited as share overall expert citations.	Same text as 2021

Appendix B: Annotated Bibliography

During the first phase of this evaluation, we conducted a systematic desk review of internal background documents from the Hewlett Foundation, earlier midstream evaluations of the Cyber Initiative, and the Camber Collective's ongoing data collection and analysis. Internal background documents included strategy articulations, grant reports, semiannual reports to the Hewlett Board, and previously commissioned field scans. We also reviewed and summarized Hewlett's Cyber Initiative grants data from the Foundation's Salesforce database.

This appendix includes a complete list and summaries of the key materials we reviewed for the analysis.

Hewlett Cyber Initiative Internal Memos (2014–2022)

The Hewlett Cyber Initiative team produced annual Internal Memos to communicate Initiative accomplishments, challenges, learning, and plans to the Foundation Board. Each memo provides the most Board-relevant information from the prior grant year, such as progress toward implementation markers, descriptions of new grantees, results and learning from research and evaluation, and any strategy shifts.

We reviewed the following **board memos**:

- Hewlett Foundation. (2014, March 2). *Cybersecurity: The State of the Field and Hewlett's Potential Impact*. Unpublished internal document.
- Hewlett Foundation. (2014, November). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2015, September 16). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2016). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2016, March). *Cyber Initiative: Refined Grantmaking Strategy*. Unpublished internal document.
- Hewlett Foundation. (2017, October 16). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2017, November). Program Budget Memo: *Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2018, August). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2019, August). *Program Strategy Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2019, October). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2020, October). *Program Budget Memo: Cyber Initiative*. Unpublished internal document.
- Hewlett Foundation. (2022, November). *Program Strategy Memo: Cyber Initiative*. Unpublished internal document.

Internal Data Source

We analyzed **grant data from the Foundation's internal grants management Salesforce database**.

- Hewlett Foundation Grants Management Software. (2022). *Cyber Grants Over Time*. Unpublished internal database.

Evaluation & Other Commissioned Reports

Starting in 2017, Camber Collective administered a **comprehensive survey to grantees** to provide Hewlett Cyber Initiative staff with a consistent way to report on grant-funded progress, budget updates, and progress toward implementation markers. Camber Collective also administered a survey to field experts to share their perceptions of grantees and to assess the relative importance of different topics or issues in the Cyber field.

Hewlett Cyber Initiative staff used the results to refine strategy and understand the Initiative's impact. We reviewed the following **materials from Camber Collective**:

- Camber Collective. (2018). *Hewlett Cyber Initiative: Grantee reporting and survey results.* Unpublished internal document.
- Camber Collective. (2019). *Hewlett Cyber Initiative: Grantee reporting and survey results.* Unpublished internal document.
- Camber Collective. (2020). *Hewlett Cyber Survey Analysis for Implementation Markers.* Unpublished internal document.
- Camber Collective. (2021). *Cyber Initiative 2020 MLE Summary Deck.* Unpublished internal document.
- Camber Collective. (2022). *Cyber Initiative 2021 MLE Summary Deck.* Unpublished internal document.
- Camber Collective. (2023). *Cyber Initiative 2022 MLE Summary Deck.* Unpublished internal document.

In 2018 The Hewlett Foundation began collecting **demographic data from grantees** about their board, staff, and senior leadership members (excluding grantees outside the US due to different contexts and understandings of demographic categories). The survey asks about race/ethnicity and gender. Grantees were required to complete the survey before receiving grant funding from the Hewlett Foundation, though they could decline to respond to specific questions. The demographic report reviewed for this evaluation includes results from 2018, 2019, 2020, and 2021 for all Hewlett Foundation grantees, with Cyber Initiative grantees disaggregated from the whole. Results show that Cyber Initiative grantees have a higher proportion of male and white board, staff, and senior leadership members as compared to the overall Hewlett Foundation grantee pool. Cyber Initiative staff used these results to inform their approach to diversity, equity, and inclusion. We reviewed the following **demographic reports**:

- The Center for Effective Philanthropy. (2020). *The William & Flora Hewlett Foundation 2019 Demographics Report – Cyber.* Unpublished internal document.
- The Center for Effective Philanthropy. (2022). *The William & Flora Hewlett Foundation 2021 Demographics Report – Cyber.* Unpublished internal document.

Camber Collective. (2016). Evaluation of Network Building: Grants & Beyond-Grant Activities. *The William and Flora Hewlett Foundation.* https://www.hewlett.org/wp-content/uploads/2018/02/Evaluation-of-network-building-Cyber-2018.pdf

Finalized in November 2016, the Camber Collective's evaluation report served as a midpoint evaluation, situated roughly two years through the then-five-year Initiative. The report drew on three main sources: (1) grant and grantee descriptions, reporting, and other materials, (2) over 40 hours of interviews with more than 30 grantee and non-grantee experts, and (3) evidence and insights from Camber Collective's additional network mapping, cyber policymaking case studies, and field/network building cases studies, to answer six questions:

1. Which of CI's [Cyber Initiative's] activities/approaches are currently working? Where are the early signs of success?
2. Is CI (through its grantees) informing cyber policymaking? What direct/indirect paths are most important?
3. What is not working? What is off track, why? What have CI and its grantees tried that has failed, in part or in whole?
4. Is CI missing anything big? Are there areas of network building to inform policy CI is note active in, but should be?
5. Has CI made any core assumptions (stated or implied) that we now have reason to question?
6. What more can CI learn about questions surfaced from the project's network building cases studies and cyber network mapping (e.g., Are translators between experts and policymakers key, and how can more be created)?

The Camber Collective developed a set of network maps using Kumu software to accompany the evaluation report by drawing upon publicly available data (e.g., congressional hearings data, conference speaker data, trusted media) as well as grantee documentation and other sources.

The results of Camber's network analysis prompted the Cyber Initiative to refine its grantmaking strategy (to explore funding organizations outside the US, provide larger grants to fewer institutions to avoid spreading the strategy too thin), refresh the Initiative's overall strategy, and help make the case for extending the Initiative's duration from 5 to 10 years with increased funding.

RTI International. (2017). Understanding Demand for Cyber Policy Resources. *The William and Flora Hewlett Foundation.* https://hewlett.org/wp-content/uploads/2017/06/RTI-report-on-understanding-demand-for-cyber-policy-resources.pdf

In this report, RTI International assessed the demand for cyber policy resources, issues, and communication across academia, civil society, and government. This report informed the Initiative's midpoint strategy refresh. Of primary concern were questions about how non-governmental members of the cyber policy community could make their work most useful and best communicate their recommendations to policymakers, as well as how government officials could best communicate their policy needs to those working on cyber policy outside of government. RTI conducted interviews with 39 current and former federal government officials in cyber policymaking roles and 15 state government officials involved in cyber policymaking in California and Washington State.

Recommendations provided in the report helped inform a key objective in the Cyber Initiative's strategy refresh: to support communication infrastructure and translation that would make cyber policy ideas and solutions accessible to the public and key decision-makers. The study also reconfirmed the importance of catalyzing additional funding and supporting multidisciplinary experts, both of which remained part of the Initiative strategy throughout.

Aday, S. (2018). Covering Cyber: Media Coverage of Cyber Issues Since 2014. Institute for Public Diplomacy and Global Communication, *George Washington University*.

Aday, S. (2020). Covering Cyber: Media Coverage of Cyber Issues: 2019-2020. Institute for Public Diplomacy and Global Communication, *George Washington University*.

The "Covering Cyber" studies analyze coverage of cyber-related issues in newspapers and network newscasts. They include an analysis of variables such as the number of cyber-related stories, how substantive the stories were, the main topics included, categories of sources quoted, and, where relevant, who was narratively positioned in the role of "villain" in the stories.

Aday, S. (2020). Verify Workshop Analysis: Assessing Outcomes from Hewlett's Cyber-Journalism Training Program. *The William and Flora Hewlett Foundation.*

Sean Aday's report on the 2018 Verify Workshop uses before and after metrics to assess the degree to which Hewlett's cyber-journalism training influenced participating journalists' coverage of cyber-related issues. The report compares their coverage before and after the event, including the number of cyber-related stories about a theme the workshop addressed, the substantive depth, and the exploratory nature of those stories. The report also assessed the number of individuals within Cyber Initiative-funded grantee organizations cited as sources (using a Lexis-Nexis search).

Nelson, J. & McGuinness, C. (2021). The Hewlett Foundation's Cyber Talent Pipeline: An evaluation based on Equitable Evaluation Framework™ principles*. The William and Flora Hewlett Foundation.* https://hewlett.org/wp-content/uploads/2021/07/Final-Cyber-Evaluation-2021.pdf

Finalized in 2021, the evaluation of the Cyber Initiative's Talent Pipeline strategy sought to answer three key questions and several sub-questions:

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 [sic] 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?

Grounded in Equitable Evaluation Framework™ principles, the evaluation included measurement and assessment of outcomes themselves as well as an inquiry into how different populations experience which outcomes, what worked, why, and for whom. Evaluators interviewed Hewlett staff, people from grantee and non-grantee universities, cyber employers, people of color in cyber policy, and diversity equity and inclusion (DEI) experts. They found that Hewlett grantee university programs made progress toward formalized and interdisciplinary programs, but that few grantee universities pursued outcomes and actions to support diversity in cyber policy itself.

Hewlett staff used the evaluation's results to help guide DEI efforts in the Cyber Initiative's remaining years.

Lachlow, I. (2022). Diversity in the Cyber Workforce: Addressing the Data Gap. *MITRE.*
https://www.mitre.org/news-insights/publication/diversity-cyber-workforce-addressing-data-gap

The Hewlett Foundation supported MITRE in partnership with Aspen Digital to "examine the challenges associated with producing a demographic baseline of the nation's cyber workforce" through literature reviews, workshops, and expert interviews. The exploration found that major agencies collect only a few characteristics, like age, birth sex, race, disability, or a combination of these four characteristics, and argues that although it is not clear which characteristics should be assessed, ethnicity, sexual orientation, gender identity, and other characteristics are necessary to fully understand the field's demographic makeup. The report provides recommendations for how data should be collected (e.g., voluntarily and anonymously) and suggests that funding needed for data collection efforts would best be provided by the US government.

Camber Collective. (2023). Cyber Funding Landscape Summary. Unpublished report.

As the Cyber Initiative was sunsetting, the Hewlett Foundation commissioned Camber Collective to conduct a funder landscape scan of select, large funders in the cyber field. This report describes cyber-related funding trends between 2018 and 2023, provides Hewlett with insight into peer funders' cyber-related funding, and leaves grantees with information about potential funders who could help fill the gap Hewlett leaves as the Initiative comes to an end.

Appendix C: Reflections on the Strong Field Framework

In addition to using the Cyber Initiative's four main evaluation questions to structure our assessment, The Hewlett Foundation early on suggested Informing Change use Bridgespan's "Strong Field Framework" (**SFF** or **Framework**) as part of our evaluation.[1] While the Framework has not gained much traction in the evaluation research literature, it has been used in other evaluations, or discussions, of field-building initiatives by philanthropies.[2] The SFF appeared appropriate because, by defining the parameters of a "strong field," it seemed to provide a semi-research-based way of assessing whether the cyber field had grown and been strengthened thanks to the Initiative. Ultimately, we made the difficult determination that using the Framework's tenets did not add sufficient value to our evaluation to warrant inclusion in the report itself. The reflections offered here document our reasoning for excluding it from the primary write-up of our findings.

CYBER INITIATIVE SUMMATIVE EVALUATION QUESTIONS

1. To what extent, and in what ways, did the Initiative achieve its goal of cultivating a multi-disciplinary cyber policy field of institutions to which decision-makers can turn, and in which they and the public may place justified confidence?
2. What contributed to the Initiative's successes, and what factors inhibited or thwarted success?
3. How, and to what extent, did the Initiative contribute to elevating the profile and visibility of cyber topics and concerns in the media and the general public discourse?
4. What lessons learned through the Initiative might inform the Foundation's other grantmaking and/or other funders' choices and grantmaking processes?

The Framework is based in part on an examination of the Hewlett Foundation's 20-year (1984–2004) Conflict Resolution Program. According to Bridgespan, this program was unique in its focus on field building as well as in its length and depth of engagement, totaling "more than $160 million of support, through almost 900 grants to more than 320 organizations."

> "… the Hewlett Foundation's Conflict Resolution Program is perhaps most distinctive for the conscious 'field-building' strategy that … guided the program from its inception. At the time Hewlett's program began, the sense of a 'field' of conflict resolution was only beginning to

[1] The James Irvine Foundation & The Bridgespan Group. (2009). *The Strong Field Framework: A Guide and Toolkit for Funders and Nonprofits Committed to Large-Scale Impact.* https://irvine-dot-org.s3.amazonaws.com/documents/64/attachments/strongfieldframework.pdf?1412656138.

[2] Examples of the SFF in evaluations or discussions of field-building initiatives by philanthropies include:

- Graham P.W., McDaniel, M., Wisniewski. R., Hawkins, S., Ramirez, D., & Baker, B. (2020). *Evaluation of the Forward Promise Initiative.* http://mcs-connect.org.s3.amazonaws.com/sbl/ForwardPromise/assets/ForwardPromise_Overall_Evaluation_Report_FINAL_12.31.20.pdf;
- Kelly, T., Brown, P., Yu, H. C., & Colombo, M. (2019). Evaluating for the Bigger Picture: Breaking Through the Learning and Evaluation Barriers to Advancing Community Systems-Change Field Knowledge. The Foundation Review, 11(2). https://doi.org/10.9707/1944-5660.1469
- Farnham, L., Nothmann, E., Tamaki, Z., & Daniels, C. (2020). *Field Building for Population-Level Change: How funders and practitioners can increase the odds of success.* https://cdn.givingcompass.org/wp-content/uploads/2020/05/06094006/Field-Building-for-Population-Level-Change.pdf.

> emerge. Hewlett support … helped to establish conflict resolution as a vibrant and sustainable field of both academic study and professional practice … Among foundation programs, there [were in 2005] few, if any, comparable examples of field-building on this scale, or of the unique relationship that developed between the Hewlett Foundation and the conflict resolution field."[3]
>
> **– DAVID KOVICK, AUTHOR**
> **THE HEWLETT FOUNDATION'S CONFLICT RESOLUTION PROGRAM — TWENTY YEARS OF FIELD-BUILDING 1984–2004**

In addition to the fact that both the Conflict Resolution Program and Cyber Initiative had the purpose of field-building in a space where a "field" was early in its emergence, both also provided general operating support grants over multiple years and participated in infrastructure building to promote nationwide knowledge, education, and training.[4] Initially, these and other similarities between the two Hewlett undertakings seemed to make the Framework well-suited to our assessment of the Cyber Initiative by providing a tool for assessing a "field's state of evolution and its strengths and needs" which appeared to be exactly what we needed.[5]

The Framework comprises an umbrella definition of "shared identity" and four additional defining dimensions of a strong field, each of which may be evaluated using 2–4 indicators:[6]

SHARED IDENTITY: COMMUNITY ALIGNED AROUND A COMMON PURPOSE AND A SET OF CORE VALUES

Standards of Practice	Knowledge Base	Leadership & Grassroots Support	Funding & Supporting Policy
• Codification of standards of practice • Exemplary models and resources (e.g., how-to guides) • Available resources to support implementation (e.g., technical assistance) • Respected credentialing/ ongoing professional development training for practitioners and leaders	• Credible evidence that practice achieves desired outcomes • Community of researchers to study and advance practice • Vehicles to collect, analyze, debate, and disseminate knowledge	• Influential leaders and exemplary organizations across key segments of the field (e.g., practitioners, researchers, business leaders, policymakers) • Broad base of support from major constituencies	• Enabling policy environment that supports and encourages model practices • Organized funding streams from public, philanthropic, and corporate sources of support

We quickly determined Initiative staff had not used the Framework to conceive of the field it sought to strengthen, and that a more academic definition of "field" was at play. This isn't surprising given the topic and Hewlett President Larry Kramer's then-recent arrival direct from Stanford Law School. Subsequently, neither the Camber Collective's annual surveys nor other prior evaluation reports on Initiative progress used the

[3] Kovick, D. (2005). *The Hewlett Foundation's Conflict Resolution Program: Twenty Years of Field-Building. 1984-2004. The Hewlett Foundation.* https://hewlett.org/library/the-hewlett-foundations-conflict-resolution-program-twenty-years-of-field-building/
[4] Kovick, D. *The Hewlett Foundation's Conflict Resolution Program.*
[5] The James Irvine Foundation and The Bridgespan Group. *The Strong Field Framework.* 4.
[6] The James Irvine Foundation and The Bridgespan Group. *The Strong Field Framework.* 4-5.

Framework's elements or many of its indicators to track the performance of grantees or assess the portfolio.[7] Still, upon first consideration, the field elements described in the SFF seemed useful for our purposes.

After determining grantees had not been asked about SFF-related perceptions in prior evaluation reports, we incorporated questions about shared identity, standards of practice, and funding and supporting policy in our interview protocol as well as in a request fulfilled by the Camber Collective to include a set of SFF-related questions in their final annual survey of grantees. We elected to exclude the **Leadership and Grassroots Support** elements from our data collection as these seemed more appropriate to an advocacy campaign. All interview and survey questions are included at the end of this **Appendix E** of the report.

As answers to our SFF questions rolled in, and our understanding of grantees' work deepened, we began to question the relevance and utility of the Framework for a few reasons. Chief among them was that the overarching umbrella dimension of **Shared Identity** simply didn't apply. As our interviews with academic grantees reminded us, the very purpose of academia is to foster free exchanges of ideas and multiple points of view. While researchers of single disciplines might be said to share a sense of identity based on that discipline, this Initiative was interdisciplinary by design. The Hewlett Foundation clearly fostered a sense of community among many of its grantees built around a common but very multifaceted topic of interest, rather than a common purpose. Given the intentionally multidisciplinary and nonpartisan makeup of the Initiative's portfolio, it would have been remarkable to find evidence that this community shared a core set of values. Definitionally, this cyber field's practitioners do not share a meaningful sense of identity in the sense articulated by the SFF.

Similarly, our data did not support the claim that this field shares many elements of shared **Standards of Practice** or **Funding and Supporting Policy**:

- While some articulations of cybertechnology ethical standards are beginning to emerge, these are far from codified in the US. A handful of exemplary models and resources have been created by Hewlett grantees, but "available resources to support implementation" are still limited, at best.
- The Initiative was created in part because there is little to no "enabling policy environment" to support and encourage the development and spread of model practices. While a key goal was to approach this absence by first helping generate a healthy pipeline of individuals who could staff and inform such an environment, it was not realistically within the Initiative's reach to generate one. Finally, although some grantees have been successful at generating additional funding for themselves thanks to Hewlett support, there is nothing that could be described as an "organized funding stream."

However, the Initiative was clearly successful at creating one element of the Standards of Practice dimension: "respected credentialing" programs led by and for practitioners and leaders. It was similarly effective at supporting most elements of the **Knowledge Base** criterion: a "community of researchers to study and advance [cyber policy] practice" and "vehicles to collect, analyze, debate and disseminate knowledge."

We also considered iterations on Bridgespan's original SFF, such as those applied or elaborated in the 2016 publication, "Building a Field: Blue Shield of California Foundation's Strong Field Project Leaves a Legacy and Valuable Lessons," and Bridgespan's later (2020) report, "Field Building for Population-Level Change: How funders and practitioners can increase the odds of success."

We did find the Blue Shield of California Foundation's (**BSCF**) definition of a "field" to be more satisfactory and better fitting than that provided by the SFF:

[7] While not referencing the Framework, the Camber Collective's annual survey of grantees did ask questions that generated data we could use to assess the degree to which the field could be characterized by indicators such as "respected credentialing/ ongoing professional development training for practitioners and leaders."

TWO DEFINITIONS OF A FIELD

The Strong Field Framework	Blue Shield of California Foundation's Strong Field Project
"A community of organizations and individuals: • Working together towards a common goal, and • **Using a set of common approaches to achieving that goal."**	"A field is defined as a branch of knowledge, policy, and practice composed of a multiplicity of actors in relationship with each other. It involves both knowledge and action. Actors in a field produce facts, solutions to problems, models of good practice, and messages to help people grasp the dimensions of a problem and promote desired changes. Field actors form a community whose members play different and complementary roles in solving social problems—advocates, program developers and implementers, communicators, leaders, organizers, researchers, policymakers, funders, and others."[8]

However, none of the iterations we investigated really addressed the mismatch we were seeing in our extensive data on the Cyber Initiative. Even BSCF, with its more detailed and nuanced definition of a field, focused its attention on public health *campaigns* where contributing to coordinated advocacy is the ultimate goal.[9] Even if some of the Hewlett convenings created conditions to facilitate networking, which, in a small number of cases, was a precursor to eventual coordination among small subgroups, the Cyber Initiative's purpose was never intentionally to help coordinate the work of grantees.

Thus we were confronted with a choice: apply an ill-fitting framework and declare this field building Initiative poor-performing on the grounds that it met, at best, fewer than half the SFF's criteria defining a strong field, or accept what our evidence was showing us: 1) the Cyber Initiative accomplished a great deal and is widely viewed by field experts as having been very successful at catalyzing a nascent *intellectual* field of multidisciplinary cyber policy experts, as well as a pipeline into that field; and 2) the SFF is not an appropriate tool for assessing this kind of field.

In arriving at the second choice, we were prompted to re-examine the Hewlett-related origins of the SFF. The problems motivating the Conflict Resolution Program were far more general and long-standing than those rapidly developing in cyber policy, to wit: "defective decision-making processes … that fail to address the interests of all concerned stakeholders."[10] Additionally, most Conflict Resolution Program grantees were primarily "practitioner organizations" involved in developing "new consensus-based *approaches* to public policy and decision-making" (emphasis added) rather than grantees conducting and sharing research to *inform* policy makers about highly technical matters in the context of national and international security.[11] Grantee funding in both endeavors included attention to methods, skills, and knowledge creation. However, the Conflict Resolution Program set out to build a field around the "how" of creating policy (more methodological and skills-based in its focus), while the Cyber Initiative emphasizes specific knowledge about the "what" that both creates the need for and requires carefully considered, well-informed public policy responses.

[8] Petrovich, J. (2011). Exiting Responsibly: Best Donor Practices in Ending Field Support. https://cof.org/sites/default/files/documents/files/RWJ%20Report%20-%20Exiting%20Responsibly%20-%20Best%20Donor%20Practices%20in%20Ending%20Field%20Support.pdf

[9] Petrovich, upon whose work the BSCF's field definition was based, states unequivocally that "implementing a range of strategies together in a coordinated and concerted fashion is what makes a field successful" (8).

[10] Kovick, D. *The Hewlett Foundation's Conflict Resolution Program.* 46. This articulation of the Conflict Resolution Program's focus emerged midway through its existence.

[11] Kovick, D. *The Hewlett Foundation's Conflict Resolution Program.* 5.

Appendix D: Evaluation Questions & Their Answers

1. **To what extent, and in what ways, did the Initiative achieve its goal of cultivating a multi-disciplinary cyber policy field of institutions to which decision-makers can turn, and in which they and the public may place justified confidence?**

   In sum, The Cyber Initiative invested in four main focus areas: 1) academic institutions; 2) think tanks and other civil society organizations; 3) communications and translation infrastructure; and 4) DEI-related efforts. Main Initiative tactics included grantmaking (both broad and focused), convenings, technical assistance, and staff thought partnership.

   Our interviewees widely agreed that changes in the field are in part a result of "the moment" and the context of a quickly evolving cyber field, and in part due to facilitative and accelerating efforts by Hewlett. Our interview data combined with prior years' Camber survey data, provide evidence that the Initiative contributed to cultivating a multi-disciplinary cyber policy field, yielding:

   - More conversation between experts, experts and journalists, and experts and policy makers;
   - More professionals taking cross-disciplinary approaches or contributing to cross-disciplinary research and dissemination;
   - Less field fragmentation according to some interviewees; others observed *increasing* silos but attributed these to the expansion of subfields within the broader field;
   - And increased awareness of the complexity and importance of cyber issues by government, media, industry, and members of the public.

   1a. To what extent have Initiative-funded institutions become more holistic and multidisciplinary in their approaches to cyber policy? Are they, consequently, better able to contribute to informed policy debate?

   Interviewees describe a greater openness to and observation of more collaboration across disciplines and specific areas within the cyber policy field. The evaluation was not able to determine the extent to which interviewees contributed to informed policy debate, in part because they were unwilling or unable to talk about the influence they may have had (or seen others have) on policymakers due to confidentiality concerns. Much policy work occurs behind the scenes and its effectiveness often depends upon confidentiality. That said, we did find evidence in 12 interviews, and in Camber survey data and Hewlett Board Reports that such contributions were occurring.

   1b. Did Initiative grantees translate and disseminate information about cyber policy, supported by Initiative funding?

   Data collected by the Camber Collective over the life of the Initiative suggest that all civil society (non-academic) grantees contributed to cyber debates, including those about five pressing categories of concern: infrastructure protection, emerging technology, information privacy, international cyber norms, and cyber warfare.

   Grantees engaged in roundtables; published research, papers, and other media; created unpublished materials; informally consulted; provided congressional testimony, and had staff or students move into government roles requiring translation and/or dissemination of cyber policy information.

1c. Are cyber policy decision makers and influencers better informed about cyber policy, thanks, at least in part, to the work of Initiative-supported grantees?

Interviewees' assessments of whether and to what degree these overall improvements in communication have led to increased understanding of cyber among policymakers and the public are mixed. Some are reluctant to make claims based on experience and anecdotal evidence alone; others don't feel well-enough informed to speak about the Initiative as a whole. Initiative funds were used to connect experts to journalists and policy makers and provided training and communication assets to journalists and policy makers to better inform them on the issues. There is anecdotal evidence that these connections are closer than they were prior to the Initiative. Survey and other data documenting publications by think tanks and others, intended for policy audiences, together with interview accounts, strongly indicate that policymakers now have more accessible information at their fingertips thanks in part to the Initiative. However, without baseline data on how well specific policymakers (or types of policy makers) understood cyber issues before the Initiative, it is difficult to say with certainty how much their levels of understanding have changed.

1d. How do grantees value and prioritize diversity, equity, and inclusion?

Grantees think about diversity expansively. In interviews, they named multiple vital dimensions of diversity, many of which grantees address in their work, including race, gender, class (and caste for India), education level, geography, age, political ideology, disability and neurodiversity, and academic discipline.

Multiple interviewees noted that often, DEI efforts within their organizations start and end at hiring and having a diverse staff/board without thinking more critically about equity or inclusion as lenses within the work itself or a value that is integrated throughout their organizations. Diverse staff is a great first step, they said, but just the beginning of the journey.

1e. To what degree, if at all, have Initiative grantees successfully sought and acquired additional new funding for their work?

Across the portfolio, reliance on Hewlett Cyber Initiative funding has decreased, year over year. However, of those grantees who responded to budget-related questions in the final 2023 Camber Collective grantee survey, nearly half (10 out of 19) will lose 50% or more of their funding once Hewlett exits the field.

1f. What unexpected positive or negative outcomes, if any, have resulted from the Initiative's strategies?

Answers to this question are integrated throughout the report.

2. What contributed to the Initiative's successes and what factors inhibited or thwarted success?

Answers to this question are discussed throughout the report.

2a. How did the Initiative's definition and articulation of the field of interest (e.g., cyber policy, broadly defined) and their specific goals impact progress? Whom did the definition include or exclude?

While interviewees do not necessarily apply the same definition and articulation of the cyber policy field in their own work, most agreed that the broad definition allowed for the Cyber Initiative to be nimble and adaptable to both external events and changing grantee needs. However, many acknowledged that there are interconnected subfields within this broad definition that may not use a shared language or have common problem sets or goals. More detailed answers to this question are offered in the report.

3. How, and to what extent, did the Initiative contribute to elevating the profile and visibility of cyber topics and concerns in the media and general public?

3a. What internal and external factors or events supported or inhibited success?

Media coverage of cyber topics and the public's awareness has increased since the start of the Initiative. While most interviewees believe that cyber and technological prevalence, advancements, threats, and warfare catalyzed the public's awareness, there is evidence that the Initiative contributed to journalistic development via the Verify Conference and grantees' work. Interviewees also named Hewlett staff as instrumental in elevating the need for more attention to cyber topics among their networks.

4. What lessons learned through the Initiative might inform the Foundation's grantmaking processes and/or other funders' choices and grantmaking processes?

Answers to this question are woven throughout the report and can be found in the report section "Lessons from & Reflections on the Cyber Initiative's Approach."

4a. What can interested funders learn from the Initiative's successes and challenges?

Answers to this question are woven throughout the report.

4b. How sensitive and responsive to grantees' contexts and needs was the Cyber Initiative? In what ways did this support or inhibit progress toward the Initiative's goals?

Grantees praised the staff of the Cyber Initiative for their thought partnership and leadership within the field, and many had examples of Cyber Initiative grantees collaborating with staff on new directions or ideas. General funding served grantees well, allowing them to focus on their grant-funded work and use funding in the ways that served their needs best. This question is further discussed within the report.

Appendix E: Evaluation Approaches, Methods & Data Collection Tools

This summative evaluation utilized a mixed-methods approach, combining and triangulating analysis of quantitative and qualitative data. Most quantitative data and a small portion of the qualitative data we analyzed was collected by the Camber Collective via annual surveys from 2017–2023. Informing Change gathered the lion's share of qualitative data via interviews.

Four main questions guided the summative evaluation:

1. **To what extent, and in what ways, did the Initiative achieve its goal of cultivating a multi-disciplinary cyber policy field of institutions to which decision-makers can turn, and in which they and the public may place justified confidence?**
    a. To what extent have Initiative-funded institutions become more holistic and multidisciplinary in their approaches to cyber policy? Are they, consequently, better able to contribute to informed policy debate?
    b. Did Initiative grantees translate and disseminate information about cyber policy, supported by Initiative funding?
    c. Are cyber policy decision makers and influencers better informed about cyber policy, thanks, at least in part, to the work of Initiative-supported grantees?
    d. How do grantees value and prioritize diversity, equity, and inclusion?
    e. To what degree, if at all, have Initiative grantees successfully sought and acquired additional new funding for their work?
    f. What unexpected positive or negative outcomes, if any, have resulted from the Initiative's strategies?
2. **What contributed to the Initiative's successes and what factors inhibited or thwarted success?**
    a. How did the Initiative's definition and articulation of their field of interest (e.g., cyber policy, broadly defined) and their specific goals impact progress? Whom did the definition include or exclude?
3. **How, and to what extent, did the Initiative contribute to elevating the profile and visibility of cyber topics and concerns in media and the general public?**
    a. What internal and external factors or events supported or inhibited success?
4. **What lessons learned through the Initiative might inform the Foundation's grantmaking processes and/or other funders' choices and grantmaking processes?**
    a. What can interested funders learn from the Initiative's successes and challenges?
    b. How sensitive and responsive to grantees' contexts and needs was the Cyber Initiative? In what ways did this support or inhibit progress toward the Initiative's goals?

Advisory Committee

Ensuring grantee voice in this evaluation was important for at least two reasons: (1) we and Hewlett wanted the final report to reflect as much of a sense of grantees' work as possible in a relatively short document; (2) Informing Change prioritizes participatory evaluation where feasible. Equally important to us is the countervailing priority to limit the burden our research places on grantees. Because the Initiative had already asked grantee representatives to complete, annually, a detailed, multi-hour survey for evaluative purposes, Foundation staff were keen to limit the onus of this summative assessment on grantees. Hence, beyond the interviews described below, we limited our participation asks to a few hours (for meetings and document review) from each of the 7 Advisory Committee members. We established this Committee with Hewlett staff assistance (see participant selection details in the **Interviews** section on page 3 of this appendix) to help us craft final evaluation questions and review a preliminary draft of this report. Their input and feedback has been incorporated to the best of our ability.

Advisory Committee Members

1. Frédérick Douzet, Professor of Geopolitics at the French Institute of Geopolitics (University of Paris 8); Director of the Center Geopolitics of the Datasphere (GEODE)
2. Jamil Jaffer, Assistant Professor of Law at George Mason University; Founder and Executive Director, National Security Institute; Director, National Security Law & Policy Program
3. George Perkovich, Ken Olivier and Angela Nomellini Chair Vice President for Studies at Carnegie Endowment for International Peace (CEIP)
4. Monica Ruiz, Program Manager, Senior Government Affairs Manager, Digital Diplomacy, Microsoft
5. Megan Stifel, Chief Strategy Officer for the Institute for Security and Technology (IST)
6. Steve Weber, Founding Faculty Director of the Center for Long-Term Cybersecurity (CLTC) at UC Berkeley
7. Benjamin Wittes, Lawfare Editor in Chief; Senior Fellow in Governance Studies at the Brookings Institution

EVALUATION DATA SOURCES & DATA COLLECTION METHODS

Desk Review & Interim Report

During the first phase of this evaluation, we conducted a systematic desk review of internal background documents from the Hewlett Foundation, earlier midstream evaluations of the Cyber Initiative, and the Camber Collective's ongoing data collection and analysis. Internal background documents included strategy articulations, grant reports, semiannual reports to the Hewlett Board, and previously commissioned field scans. We also reviewed and summarized Hewlett's Cyber Initiative grants data from their Salesforce database as of August 2023, as well as a 2023 budget spreadsheet to approximate the planned grants through the end of 2023.

Thanks to Camber Collective's annual grantee and expert surveys, as well as a midpoint Cyber Initiative network analysis, existing data about the Initiative's implementation markers were plentiful when we began this project. Additionally, Camber Collective administered a final, pared down, annual survey during the winter of 2023, providing snapshots of the Initiative's progress toward specific measures over time.

The Initiative's earliest measures were written in 2015. They focused on five core outcomes, including 1) building the capacity of civil society organizations, 2) building the capacity of decision-makers and influencers, 3) building a robust network of experts, 4) generating policy-relevant research and thought leadership, and 5) catalyzing additional funding. When Cyber Initiative staff refreshed their strategy in 2017, they narrowed their focus into three pillars: (1) building a set of core institutions with sufficient depth of expertise to deliver solutions that take competing values and trade-offs to pressing cyber-policy challenges seriously; (2) creating a talent pipeline that produces experts with the necessary mix of technical and non-technical skills and knowledge to staff these and other institutions, including government and industry; and (3) supporting the development of infrastructure to translate and disseminate the work of these institutions into forms that can be used by decisionmakers and understood by the public. (See **Appendix A** for a full list of outcomes and implementation markers over time.)

They also introduced an accompanying monitoring plan that included 20 short-term (1–2 years) and 22 longer-term (3–5 years) targets, as well as 10 related implementation markers across the three Initiative strategies. The Camber Collective measured progress toward these targets and implementation markers annually via a grantee survey as well as a survey for other experts in the field. We conducted a point-by-point comparison of each measure, starting with the earliest measures written in 2015, using data collected via the Camber Collective-

administered surveys, prior evaluation and research reports that the Foundation commissioned, and additional background materials. This review allowed us to determine the degree to which existing data addressed each measure, which measures would require new data to gauge the portfolio's success, and which had proven less useful (or more difficult to document) according to Hewlett and Camber Collective staff.

Based on our analysis of this data trove, we produced an interim draft report in early 2023, summarizing our understanding of the project's goals and outcomes to date, evolution, and funding streams. This permitted us to test our understanding of the Initiative, including its origins, strategies, and shifts with Hewlett staff; it also gave staff an opportunity to ensure our emphases were well-aligned with the Foundation's learning and documentation interests. Together, the iterative drafting and discussion processes enabled us to focus our efforts on the summative evaluation questions that required additional qualitative data, such as: How do grantees value and prioritize diversity, equity, and inclusion? What contributed to the Initiative's successes and what factors inhibited or thwarted success? How did the Initiative staff's definition and articulation of their field of interest and specific goals impact progress? Whom did the definition include or exclude?

Appendix B includes a complete list and summaries of the key materials we reviewed for the analysis.

Interviews

To fill the qualitative data gaps, we conducted 44 original interviews with four stakeholder groups: Hewlett Foundation staff and consultants to the Initiative (8 staff and 5 consultants), Initiative grantees (21 individuals representing 20 organizations), field experts (8), select staff from other funders with current, previous, or potential investments in the field (4 peer funders).[1]

We selected **grantees** to provide representation across a handful of key variables: the year the grantee organization first received an Initiative grant; geographic location (US or international, plus representation across the US); and institution type (think tank, university, other), with the additional goal of ensuring our interview pool had gender and ethnic/racial diversity.[2] We included representatives from all anchor grantees and MSI grantees in the interview pool. To a limited extent, we additionally used snowball sampling, reaching out to or lightly researching additional grantees based on the recommendations from the initial pool of interviewees.

While Hewlett Foundation staff assisted us with developing this pool by providing a long list of names, institutions, and contact information, they did not attempt to control our selections from the list. They did however recommend individuals for our **Grantee Advisory Committee**, keeping the same variables in mind; and when we had no relevant basis upon which to choose among small groups of individuals from larger organizations, they identified for us the individuals whom they thought would be most informed about that grantee's work and best suited to answer our questions.

To generate the **field expert** interview pool, we first reviewed the roster of field experts who had previously responded to the annual Camber Collective experts survey. In consultation with Initiative staff, we generated an interview pool that included experts working in government, academia/universities, and journalism. While we attempted to interview individuals working in for-profit cyber industries, none responded to multiple invitations.

[1] The sum of persons interviewed (46) exceeds the total number of interviews (44) because not all interviews were conducted with a single individual.

[2] In keeping with Informing Change's commitment to equitable evaluation and given the dramatic underrepresentation of women and people of color in the cyber field generally—as well as a near-fully representative body of data from the Camber Collective surveys—we over-sampled for these groups. That is, we interviewed a slightly higher percentage of women and people of color than was statistically representative of the grantee pool. The Hewlett Foundation assisted us in this effort by working to ensure that where their grantee organizations had women and people of color on staff, these contacts were included in the list they provided to us.

Finally, we created a small interview pool of **staff from peer foundations** by again consulting with Initiative staff. They identified for us foundations and individual donors within their network who currently support or have previously funded cyber-related work, or that, in Hewlett's estimation, are potentially interested in doing so.

Following each interview, Informing Change provided interviewees with their interview transcripts to review them for accuracy or to identify responses they preferred us not to include in our reporting. We also confirmed their permission to include all verbatim quotes included in the final report.

We analyzed all interviews using the qualitative analysis software Dedoose. We coded both for answers to specific evaluation and other interview questions, as well as emergently, then iteratively analyzed the data for common themes. We conducted a formal intercoder reliability test as coding began and informally checked coding consistency and accuracy between rounds of individual and team analysis.

Survey

We included a brief set of **survey questions** in Camber Collective's 2023 annual survey of current grantees (i.e., organizations that received grants in 2022). In total, we received 42 survey responses, including those from 20 civil society organizations and 22 academic institutions. Every grantee who was sent the survey responded, with the exception of 3 grantees who were considered exempt. These data were analyzed in Excel.

The survey questions focused on measures related to the James Irvine Foundation-funded, Bridgespan "Strong Field Framework"(**SFF** or **Framework**).[3] We incorporated questions about shared identity, standards of practice (i.e., ethics), and funding and supporting policy which we then analyzed according to these criteria of a "strong field." However, when the analysis proved less useful than expected, we did not report our data in terms of these criteria (see more in **Appendix C: Reflections on the Strong Field Framework**).

All survey questions are included in this appendix.

[3] The James Irvine Foundation & The Bridgespan Group. (2009, June). *The Strong Field Framework: A Guide and Toolkit for Funders and Nonprofits Committed to Large-Scale Impact.* https://irvine-dot-org.s3.amazonaws.com/documents/64/attachments/strongfieldframework.pdf?1412656138

DATA COLLECTION TOOLS

2023 Grantee Survey Questions Appended to Annual Camber Collective Survey

While other sections of the survey cover the 2022 calendar year, this next section will ask questions about the current cyber policy field *as of 2023* or the Cyber Policy Initiative *as a whole*.

1. The "Strong Field Framework" (as defined by Bridgespan and the Irvine Foundation) lists specific criteria to determine whether something constitutes a field.

   The Cyber Initiative defines the field of '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.

   Please indicate below whether you believe the cyber policy field (defined above) meets each criterion today in 2023.

CRITERIA	WOULD YOU SAY EACH OF THE FOLLOWING ARE TRUE OF WHAT HEWLETT DEFINES AS THE CYBER POLICY FIELD AS OF 2023			
	No	In part	Yes	Don't Know or NA
Shared Identity - *Community aligned around a common purpose and a set of core values*	○	○	○	○
Standards of practice - *Codification of standards of practice* - *Exemplary models and resources (e.g., how-to-guides)* - *Available resources to support implementation (e.g., technical assistance)* - *Respected credentialing/ongoing professional development training for practitioners and leaders*	○	○	○	○
Knowledge Base - *Credible evidence that practice achieves desired outcomes* - *Community of researchers to study and advance practice* - *Vehicles to collect, analyze, debate, and disseminate knowledge*	○	○	○	○
Leadership and Grassroots Support - *Influential leaders and exemplary organizations across key segments of the field (e.g., practitioners, researchers, business leaders, policymakers)* - *Broad base of support from major constituencies*	○	○	○	○

Funding and Supporting Policy - *Enabling policy environment that supports and encourages model practices* - *Organized funding streams from public, philanthropic, and corporate sources of support*	○	○	○	○

2. Considering the criteria above, what do you think has been Hewlett's **most significant contribution** to the development of a cyber policy field through the Cyber Policy Initiative?
   [Open-ended response]

3. To what extent do you disagree or agree with the following **premises underlying Hewlett's Cyber Initiative**?

	STRONGLY DISAGREE	DISAGREE	NEITHER DISAGREE NOR AGREE	AGREE	STRONGLY AGREE	DON'T KNOW OR NA
a. Increasing disciplinary diversity in the field leads to better-informed policy recommendations.	○	○	○	○	○	○
b. Increasing disciplinary diversity in the field leads to improvements in how cyber policy recommendations are communicated to policymakers.	○	○	○	○	○	○
c. Increasing racial diversity in the field will lead to better-informed policy recommendations.	○	○	○	○	○	○

4. Please indicate the extent to which you disagree or agree with the following statement about **how funding was structured** for this initiative. Please consider all funding you have received through the Cyber Policy Initiative, regardless of what year the grant was given.

   Note: We define funding structure as the application and reporting requirements together with regulations related to how funding may be utilized or spent.

   The structure of Hewlett's Cyber Initiative grant(s) to me/my organization provided the flexibility needed to approach the work effectively.
   - ○ Strongly disagree
   - ○ Disagree
   - ○ Neither disagree nor agree
   - ○ Agree
   - ○ Strongly agree
   - ○ Don't know or NA

5. Please elaborate or provide an example that helps explain your response to the question above.

Grantee Interview Questions

Background

1. Please briefly describe how you came to be engaged with the Hewlett Foundation's Cyber Initiative and tell me a little about the work that you [and your organization/department] do related to cyber policy.

Defining the field

2. In the initiative, 'cyber policy' has been broadly defined 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.
    a. Do you think most cyber policy experts would agree with this definition?

3. Given this definition and where you sit within that ecosystem, how interconnected do you feel with the field at large?

4. At the onset of the initiative, the Hewlett Foundation identified three key problems in the field: (1) the field was fragmented, making it difficult for relevant actors to work together;(2) the field lacked thought leadership that could keep pace with fast-changing policy decisions and other developments; and (3) the technical nature of the issues made the threats difficult for the general public and policymakers to understand.
    a. To what extent do you think the initiative has been successful in addressing or making inroads toward addressing these three key problems?

5. If the field were successful beyond your wildest dreams, what would it [the field] look like in 10 years?

Initiative's progress: Talent Pipeline

6. From your perspective, was the initiative successful in creating a **talent pipeline** of experts with the necessary mix of technical and nontechnical skills and knowledge to staff cyber policy positions in government, industry, and the social sector?
    a. **[IF YES]** What do you think most contributed to its success?
    b. **[IF NO]** What do you think most hindered its ability to do so?

7. As the initiative ends, how well-positioned is the field to continue building that pipeline or advancing people through existing pipelines? Why or why not?

Initiative's progress: Strong Institutions

8. In what ways have the initiative's efforts to strengthen institutional capacity to inform public policy enabled or hindered its grantees' capacity to do so?
    a. What do you think most contributed to those positive/negative changes? (e.g., media and communications training, convenings, etc.)
    b. What, if anything, hindered the initiative's ability to (further) succeed?

Research & Communications

[Ask 9 and 10 of all, if time allows; but definitely ask of communications grantees and think tanks]

9. What are the strengths and weaknesses related to **communications** about cyber policy issues (e.g., communications across sub-fields, ability of the media to communicate about cyber policy, ability of key sectors to digest and communicate about cyber policy, etc.)?
    a. What factors account for these strengths and weaknesses?

10. What are the strengths and weaknesses related to the work of the **research institutions or think tanks** that focus on cyber policy topics (if relevant, including yours)?
    a. What factors account for these strengths and weaknesses?

Diversity, Equity, & Inclusion (DEI)

11. We understand the Foundation provided funding specifically to help increase [racial] diversity, equity, and inclusion (or DEI) in the cyber policy field. Although it is likely too soon to have seen the effects of these efforts, we are curious to understand to what extent you think the cyber policy field has changed or is set up to change from a DEI perspective based on that intentional investment from the Foundation?
    a. Have you received those funds, and if so, how have you used them?
        i. **[If yes and funds have been used]** What's worked well, and what has been challenging?
        ii. **[If selected for funding]** If you were in charge of funding to increase DEI in the cyber policy field, what—if anything—might you have done differently than Hewlett? What would you have recommended to better support DEI at your own institution?

    b. **[If interviewee is not from one of the DEI-grant receiving individuals or entities]** Has your own institution/organization taken any steps to increase racial diversity in the cyber policy field? If so, please tell me a bit about them.

12. In what ways or places do you think the field most needs to racially diversify, and why?
    a. What do you think are feasible changes to expect within the next 5-10 years related to DEI for the field?

Experience with the Cyber Initiative (Successes + Challenges)

13. What would you say is the most significant change to which the Hewlett Cyber Initiative contributed to in your own [work/institution/organization]?
    a. What about the Initiative played the most important role in contributing to this change? Consider funding, activities beyond the grant dollars.
    b. **[If not already addressed]** Aside from funding, what other support or resources that Hewlett provided most contributed to the initiative's success and that of your own program/organization?

14. Have you been a part of or observed collaborations with/among grantees? If so, please share more about the type of collaboration (e.g., forming partnerships, thought partnership, something else).
    a. What facilitated those efforts?
    b. What hindered those efforts?
    c. What resulted from those partnerships?

15. [If time permits] What about how funding from the Hewlett Foundation was structured was, or was not, useful that you'd want future funders to keep in mind? (In other words, what is the most effective way funders can give to grantees like you?)
    a. How, if at all, did this type of funding help overcome barriers that other funding structures may pose? What, if any, challenges did it pose?

[If time permits] Evolution of Funding and Ethical practices in the Field

16. What changes or trends, if any, have you noticed in the cyber policy funding landscape over the last 10-15 years? In other words, how has funding of the space shifted, if at all?
    a. Who are the primary actors supporting the field?
    b. From your vantage point, what are the most salient opportunities for future funders to advance cyber policy?

17. Most established fields have standards of ethical practice that evolve within or alongside the field. How have you seen the field of cyber policy deal with ethics as it has evolved?
    a. What are the most pressing issues you've seen related to ethics in the evolution of this new field?

18. What can future funders do to help develop or further the development of ethical standards of practice for a field where technological advancements are often made more quickly than the policy landscape can keep up with?

The Future

19. What advice do you have for the future supporters or contributors who want to work toward the continued development of a cohesive cyber policy field?
    Listen and probe for different types of support or characteristics of contributors, like financial support, networking, platform connections.

Closing

20. Was there anything else you'd like to share with me that none of my questions made space for?

Field Expert Interview Questions

Background

1. Please tell us a little bit about your background and areas of expertise, particularly as they relate to cyber policy or related fields.

Initiative Familiarity

2. We are conducting these interviews for the Hewlett Foundation, as part of their final evaluation of their 10-year Cyber Initiative. How familiar are you with this Initiative?
    a. **[If familiar with the Initiative]** How did you come to know of it?
    b. **[If not familiar]** Here is a brief overview of the Initiative: The William and Flora Hewlett Foundation's Cyber Initiative is a ten-year $130 million grantmaking effort that strives to build an enduring and capable cyber policy field. The Initiative's overarching goal is to "cultivate a field of institutions to which decision makers can turn and in which the public can place confidence for solutions to pressing cyber policy challenges."[4]

Evolution of the cyber policy field

3. What major trends or shifts have you noticed in cyber policy in the last 10 years?
    a. **[If not answered above]** What contributed to those shifts?

4. What opportunities (taken or missed) to improve cyber policy in the US [or internationally, if applicable] have you observed?
   As needed, probe for progress toward good/equitable/important policy changes
    a. What trends do you see on the horizon that may signal the approach of new barriers to improvement in cyber policy in the US [or internationally, if applicable]?
       As needed, probe for progress toward good/equitable/important policy changes

5. Most established fields have standards of ethical practice that evolve within or alongside the field. How have you seen the field of cyber policy deal with ethics as it has evolved?
    a. What are the most pressing issues you've seen related to ethics in the evolution of this new field?

6. What can future funders do to help develop or further the development of ethical standards of practice for a field where technological advancements are often made more quickly than the policy landscape can keep up with?

Field-building progress & the Initiative's Contribution to the field

7. **[If familiar with Initiative]** At the onset of the initiative, the Hewlett Foundation identified three key problems in the field: (1) the field was fragmented, making it difficult for relevant actors to work together;(2) the field lacked thought leadership that could keep pace with fast-changing policy decisions and other developments; and (3) the technical nature of the issues made the threats difficult for the general public and policymakers to understand.
    a. To what extent do you think the initiative has been successful in addressing or making inroads toward addressing these three key problems?

[4] Sourced from the evaluation RFP.

8. **[If familiar with Initiative]** To what extent, and in what ways, has the Hewlett Foundation's Cyber Initiative contributed to cultivating a field of institutions to which decision-makers can turn for pressing cyber policy challenges?
    a. **[If not familiar with the Initiative but is familiar with at least 1 grantee in the Initiative]** To what extent, and in what ways, would you say [this grantee/these grantees] have contributed to important cyber policy conversations?
    b. To what extent do you think they are viewed as trustworthy experts by policymakers or other decisionmakers?

9. Who, from your perspective, are the key players in the field?
    a. Are these the same people/organizations that would likely be called upon to provide viable solutions to cyber debates or events?

10. To what degree would you say that public policy around cyber issues is well-informed by relevant experts?
    a. The Cyber Initiative defines the field of '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.

11. What, or whose, voices would you say are missing in public debate about cyber policy?
    Probe for bipartisan representation; whether the habit remains for policy makers to turn to 1-2 people they personally trust for information rather than casting a wider net; whether policy makers are getting technically accurate information; etc.

12. To what extent do you think the public also places confidence in these people, the field, or institutions to develop solutions to pressing cyber policy challenges?

13. To what extent do you think technical information that should inform cyber policy is easily accessible to policymakers or the public?
    a. Can you provide examples of research that, in your view, fits this criterion?

Initiative-Specific Questions

14. From your perspective, what are the strengths and weaknesses of the current **talent pipeline** for cyber policy experts in the US? Super hit and miss.
    Probe for inter-disciplinary nature, diversity, entry into relevant jobs
    a. What factors account for these strengths and weaknesses?
    b. [If not yet mentioned] How, if at all, has the Initiative contributed to building the talent pipeline for cyber policy experts in the US?

15. What are the strengths and weaknesses related to **communications** about cyber policy issues (e.g., communications across sub-fields, ability of the media to communicate about cyber policy, ability of key sectors to digest and communicate about cyber policy, etc.)?
    a. What factors account for these strengths and weaknesses?
    b. [If not yet mentioned] How, if at all, has the Initiative contributed to improving communications related to cyber policy issues?

16. Are you familiar with the work of any research institutions or **think tanks** that focus on cyber policy topics?
    a. [If familiar] What are the strengths and weaknesses of this work?

b. [If familiar] What factors account for these strengths and weaknesses?
c. [If familiar and if not yet mentioned] How, if at all, has the Initiative contributed to think tanks that focus on cyber policy topics?

17. If you were asked to advise philanthropic foundations *today* on how best to address cyber policy issues, what advice would you give?

Closing

18. Was there anything else you'd like to share with me that none of my questions made space for?

Peer Funder Interview Questions

Background

1. Please tell us a little bit about your current institution, your role in it, and the issue areas your institution typically funds.
    a. **[If institution funds cyber or adjacent topics]** Please tell us how long you've been funding cyber, cyber-policy, or adjacent fields.

Initiative's Success in Building a Field, a Pipeline and Strong Institutions

2. Are you familiar with the Hewlett Foundation's Cyber Initiative?

    a. ***[If no]*** *Hewlett set out to develop a durable cyber policy field with three overarching goals: (1) building a set of core institutions with sufficient depth of expertise to deliver solutions to pressing cyber policy problems; (2) creating a talent pipeline that produces experts with the necessary mix of technical and nontechnical skills and knowledge to staff these and other institutions, including government and industry; and (3) supporting the development of infrastructure capable of translating and disseminating the work of these institutions in forms that can be used by decision makers and understood by the public. Then, starting in 2018, the Initiative added to its strategy efforts to improve diversity within the field.*

    b. **[If yes]** To what extent, and in what ways, do you think the Initiative has contributed to cultivating a field of institutions with deep expertise to which decision-makers can turn, and in which they and the public can place justified confidence, for solutions to pressing cyber policy challenges?

        i. More specifically, what is your sense of…
            1. The strength of institutions now contributing to the cyber policy field?
            2. The state and diversity of the talent pipeline?
            3. The degree to which decision-makers and the public can access and understand accurate information about cyber policy-related issues, such as Internet governance, net neutrality, encryption, surveillance, and privacy?

        ii. **[If not yet answered – Reminder to interviewee to return to Initiative's contributions]** From what you've observed, how did the Initiative contribute to the state of or progress on the topics we just discussed?

Evolution of Funding in the Field

3. What changes or trends, if any, have you noticed in the cyber policy funding landscape over the last 10-15 years? In other words, how has funding of the space shifted if at all?
    a. **[If mentioned increases in funding]** Where have you noticed more interest or movement in funding the cyber policy field? Why do you think that is?
    b. What role, if any, do you think funders see themselves as playing in the cyber policy field in the future?

4. Who do you see as the primary actors (not including Hewlett) funding the field today?

5. From your vantage point, what are the most salient opportunities for future funders to advance cyber policy?

6. What concerns, if any, do you have—or do you think other funders have—about funding the cyber policy field or cyber topics?
    a. What do you think could help, reassure, further encourage, or motivate funders to engage more deeply in this space or fund it?
    b. What suggestions do you have for how to optimize opportunities or mitigate barriers to ensure continued or increased funding in this space?

7. **[If answers to above indicate they can speak to trends in cyber policy]** What cyber policy or funding trends have you noticed in the past few years that might create opportunities for increased funding for cyber policy-related topics in the US or abroad?
    a. What about cyber policy or funding trends that might become barriers to increased funding of cyber policy-related topics in the US or abroad?

The Future (Hopes & Recommendations)

8. What advice do you have for the future stewards of the cyber policy space to ensure the continued development of a cohesive field?

9. Most established fields have standards of ethical practice that evolve within or alongside the field. What can future funders do to help develop or further the development of ethical standards of practice for a field where technological advancements are often made more quickly than the policy landscape can keep up with?

Closing

10. Was there anything else you'd like to share with me that none of my questions made space for?

Hewlett Foundation Staff Interview Questions

Background

1. Please tell us how, and for how long, you've been engaged with the Foundation's Cyber Initiative, and what your role is and has been.

Defining and building the field

2. How would you say Hewlett's definition of the field has changed, if at all, since the start of the Initiative?
   PROBE: If you had to describe the baseline state of the field now, what are the main ways in which it would differ from the baseline state described at the start of the Initiative? *[Very little policymaker trust in experts except those personally known to the policymaker; conviction that most experts are "biased"; sense that it's too difficult to understand experts; etc.]*

3. In the grand scheme of things, given the shifts you have noticed, to what degree do you think the Hewlett Foundation has played a role in the creation of the cyber policy field?

4. We've heard from some that the way Hewlett initially entitled the "field" for this initiative may have influenced its development (e.g., cyber-too broad; cybersecurity-too narrow; cyber policy-current). Do you think that might be the case, and if so, please say more?
   a. If you had to re-frame / re-name it now, how would you do so?

5. How would you define the main sub-fields within the Cyber Policy field?
   a. Who are the primary actors leading the field and main sub-fields?

6. Most established fields have standards of ethical practice that evolve within or alongside the field. How have you seen the field of cyber policy deal with ethics as it has evolved?
   a. What are the most pressing issues you've seen related to ethics in the evolution of this new field?

Initiative's success in building a pipeline and strong institutions

7. From your perspective, was the initiative successful in creating a talent pipeline of experts with the necessary mix of technical and nontechnical skills and knowledge to staff cyber policy positions in government, industry, and the social sector?
   a. **[IF YES]** What do you think most contributed to its success?
   b. **[IF NO]** What do you think most hindered its ability to do so?

8. As the initiative ends, how well-positioned is the field to continue building that pipeline or advancing people through existing pipelines? Why or why not?

9. What would you say have been the main changes stemming from the initiative's efforts to strengthen institutional capacity to inform public policy, whether positive or negative?
   a. What do you think most contributed to those positive/negative changes?
   b. What, if anything, hindered the initiative's ability to (further) succeed?

10. What are the strengths and weaknesses related to communications about cyber policy issues (e.g., communications across sub-fields, ability of the media to communicate about cyber policy, ability of key sectors to digest and communicate about cyber policy, etc.)?
    a. What factors account for these strengths and weaknesses?

11. Are you familiar with the work of any research institutions or think tanks that focus on cyber policy topics?
    a. [If familiar] What are the strengths and weaknesses of this work?
    b. What factors account for these strengths and weaknesses?

If the Foundation had to do things over again...

12. In retrospect, what do you think should have happened differently or what else could the Foundation have done to increase the success of the initiative overall?

Evolution of Funding in the Field

13. What changes or trends, if any, have you noticed in the cyber policy funding landscape over the last 10-15 years? In other words, how has funding of the space shifted, if at all?

14. From your vantage point, where are the most salient opportunities for future funders to advance cyber policy?

15. What concerns, if any, do you think other funders have about funding this space?
    Probe for presence or lack of bipartisan representation, trust/respect across sectors

16. What do you think could help reassure, encourage, or persuade funders to engage more deeply in this space?

Future oriented

17. What advice do you have for the future supporters or contributors who want to work toward the continued development of a cohesive cyber policy field?
    Listen and probe for different types of support or characteristics of contributors like financial support, networking, platform connections.
    a. What approaches taken by civil society actors to influence the cyber policy field (as Hewlett currently defines it) are most in need of strengthening?
    b. What can future funders do to help develop or further the development of ethical standards of practice for a field where technological advancements are often made more quickly than the policy landscape can keep up with?

Closing

18. Was there anything else you'd like to share with me that none of my questions made space for?

Cyber Initiative Consultant Interview Questions

1. Please briefly share a little bit about the work that you do and how you came to be involved with the Hewlett Foundation's Cyber Initiative.
    a. [Probe for whether they provided broad consulting services (e.g., through webinars), worked with specific grantees on an individual basis, or both]
    b. [If not answered] Are you actively or currently providing consulting services for this Initiative? For how long have you / did you provide these services?

2. More specifically, what work have you done with the Cyber Initiative grantees?
    a. [Probe for at least one concrete example]
    b. What changes have you observed in grantees, either as a result of your engagement with them, or just over the time you (have) worked with them?

3. How (and when) have you observed your engagements to be most effective for grantees?
    a. What challenges, if any, did you observe grantees having as they applied your services [tailor based on what they provide]?
    b. What, if any challenges did **you experience** in providing support to grantees?
    c. What preparation or support, if any, did the Foundation provide to you for your work with grantees?
        i. How, if at all, could they have better supported you to be more effective?
        ii. How about for grantees to make the most of their engagement with you?
    d. In retrospect, what, if anything, do you think might have made your engagements more effective?

4. From your vantage point, what are grantees' greatest strengths as they relate to [the consultant's area of expertise]?
    a. What about their greatest challenges?
    b. What additional support do you think grantees would most benefit from to be more effective at [the consultant's area of expertise]?
    c. In retrospect, which or what types of grantees that you worked with through this initiative most benefited from your support? [If not addressed above: Why do you think that was?]
    d. What other observations can you share about grantees from your work with them?

5. We'll be documenting in greater detail 5 specific case examples. If you had to pick one grantee, or cluster of grantees, that you think had the greatest success with regard to [the consultant's area of expertise], who/what would it be and why?

6. In relation to the kinds or topics of support you provided, what advice would you give to other funders interested in entering this space?
    a. What are potential areas for future funding as they relate to [the consultant's area of expertise]? In other words, how can future funders best support grantees with [the consultant's area of expertise]?

7. Is there anything else you'd like to share—or that you feel it's important for our evaluation to reflect?

INFORMING CHANGE

360 22nd Street, Suite 730
Oakland, CA 94612
510.665.6100

info@informingchange.com

informingchange.com