CAMBER COLLECTIVE

EVALUATION *of* NETWORK BUILDING

GRANTS & BEYOND-GRANT ACTIVITIES / HEWLETT FOUNDATION CYBER INITIATIVE

NOVEMBER 2016

Evaluation content was finalized in November, 2016 as part of a larger, 3-part project with the Cyber Initiative that also included network mapping and strategy refinement components. For questions about this evaluation report, please email josh@cambercollective.com

CAMBER COLLECTIVE

TABLE *of* CONTENTS

The Cyber Initiative's network building effort already has several major wins, but also a number of grant-specific challenges and areas where its underlying assumptions/strategy need refinement. On the positive side, several grants (e.g. the $380K grant to the Harvard Berkman center resulting in the influential "Don't Panic" report) are both relatively low cost and high/rapid return. These grants are breaking new intellectual ground, building trust between parts of the network that previously seldom worked together, and producing materials, events, and relationships informing policy. At the same time, the performance of some other grants—particularly the largest/longest $15M grants to MIT, Berkeley, and Stanford—have results that are less clear, partly because they need to be evaluated over a longer timeline.

The evaluation also surfaced broader insights that have less to do with the performance of any single grant and more to do with emerging evidence that certain of the Initiative's network building hypotheses (e.g. expertise exchange through fellowships) may be more effective at catalyzing trust, forming connections, and informing policy than others. Finally, the evaluation surfaced foundational questions for the Initiative to wrestle with, such as: (i) Whether the network of experts has sufficient bipartisan connections and credibility to exert influence, (ii) What the proper balance is between accepting the network as is and maximizing short-term policy impact vs. attempting to fundamentally change the network through longer-term bets like training the next generation of experts, and (iii) Whether the Initiative's broad strategy, goal, and outcomes align with its comparatively modest staff, budget, and timeframe.

I. INTRODUCTION & METHODOLOGY

Barely two years into its efforts to catalyze a network of experts informing cyber policymaking, evidence is emerging suggesting areas where the Cyber Initiative is making notable progress, as well as where it may need to adjust its strategy. Our preceding cyber policymaking case studies and broader network mapping effort confirmed there are already networks of experts, but that they are often not connected to one another and possess insights and expertise that are often not yet informing formal government and/or corporate policymaking.[1]

Our evaluation sought to answer six core questions developed with Hewlett program, strategy, and evaluation staff. With only two years of grant making and activities on this Outcome, this represents a midstream evaluation not an ex-post evaluation able to rely on grantee reporting and clearly observable impacts. This report draws from three sources: (i) grant descriptions, grantee reporting, and additional grantee documents such as policy briefs or convening agendas, (ii) 40+ hours of interviews with 30+ grantee and non-grantee experts, and (iii) evidence and insights from our additional workstreams on network mapping, cyber policymaking case studies, and field/network building cases studies.[2]

Nearly half of the Initiative's grants including network building as a primary objective are <12 months old. About a third have only one written report, and half have no written report as of November 2016. Because so little grantee reporting exists, we had to rely more on interviews and expert opinion. Roughly half of our 30+ interviewees were Hewlett grantees, while the other half were 3rd party experts able to: (i) report on Hewlett grantees' performances and/or (ii) offer broader observations about the network and Hewlett's activities to catalyze its growth and connectivity to policy debate and making.

To ensure we got candid feedback, all interviews were 100% confidential. An early list of interviewees was reviewed and developed with input from the Cyber Initiative's Program Officer Eli Sugarman, but will not be reproduced in this report or any annex.[3] The complete "interview guide" can be found in Annex 1 on pp 22-24.

We also over-sampled anchor grantees' work and experts to better understand how they are performing as individual grants, in comparison to one another, and versus other network builders. The three anchor grants are some of the Initiative's oldest as well as largest and represent about 70% of the Initiative's approved grantmaking.

HIGH-LEVEL EVALUATION QUESTIONS

- Q Which of CI's activities/approaches are currently working? Where are the early signs of success?
- Q Is CI (through its grantees) informing cyber policymaking? What direct/indirect paths are most important?
- Q What is NOT working? What is off track, why? What have CI and its grantees tried that has failed, in part or in whole?
- Q Is CI missing anything big? Are there areas of network building to inform policy CI is NOT active in, but should be?
- Q Has CI made any core assumptions (stated or implied) that we now have reason to question?
- Q 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)?

30+ INTERVIEWEES FROM ACROSS THE NETWORK

- **13** from ACADEMIA (e.g. Berkeley)
- **5** from THINK TANKS (e.g. New America)
- **5** from ADVOCATES (e.g. EFF)
- **5** from INDUSTRY (e.g. Microsoft)
- **2** from MEDIA (e.g. NYT)
- **6** from GOVT POLICYMAKING (e.g. Congress)
- **2** from MILITARY/ INTEL (e.g. NSA)
- **2** from THE "HACKER" COMMUNITY

[1] The William and Flora Hewlett Foundation commissioned this analysis as part of a broader mapping, evaluation, and strategy refinement effort for its Cyber Initiative in recognition that its network building outcome is the most important as well as hardest to achieve.

[2] Network mapping included creation of a database of network actors and connections visually displayed in online platform Kumu, as well as additional bespoke analytics. Cyber policymaking case studies summarized how policymaking current is/not working by examining three contemporary cases on: (i) U.S. response to Chinese commercial cyber espionage, (ii) Coordination of "botnet" takedowns, and (iii) IANA/ICANN transition. Field and network building cases studies examined 10 cases from fields as diverse at the conservative legal movement to climate change, distilling field and network building best practices and lessons learned for the Cyber Initiative.

[3] If a specific interviewee was credibly part of two groups (e.g. they had served in the White House and had also been in academia for >2 years) we considered them a member of both groups.

Although this paper focuses on lessons-learned to date from the Cyber Initiative's grant and beyond-grant network building activities, some of its insights may also apply to other Initiative Outcomes and/or to other field or network building efforts within and outside Hewlett. The insights in this paper progress in four stages:

- **What we have learned broadly about the operating environment in which the network is growing**
- **Where there are early signs of success from Hewlett's and others' network building activities**
- **Which activities appear NOT to be working and where there are other barriers**
- **What this means for Hewlett's strategy, its current network building activities, and how/if it should shift funding, staff time, and voice/influence moving forward**

II. OPERATING ENVIRONMENT/CONTEXT INSIGHTS

The evaluation generated insights into the broader situation and context in which Hewlett is trying to affect change. At a high level, these include:

- **Ingrained barriers within government further increase the gap between policy and technology**
- **A generational gap in technical knowledge and interdisciplinary approach; and a slow, natural path to change**
- **The importance and current role of personal networks in bringing experts into the policy discussion**
- **A lack of political diversity in the network of experts, thereby potentially limiting policy influence, particularly in DC**
- **The dominant position of corporations and their outsized influence on policy**
- **The important role played by media and public opinion**
- **An overly U.S.-centric approach in the network and by policymakers**

Government's ability to create new cyber policy is blocked by ingrained challenges.

Interviewees, like Hewlett, saw cyber policy (particularly policy made by governments) as lagging dangerously behind the technologies it was trying to influence and, in some cases, regulate. Many noted that although similar gaps have accompanied other disruptive technologies, the challenges across the field of cyber are far larger due to: (i) the pace with which innovation is taking place in the private sector, and (ii) the breadth of cyber innovations impact. As one interviewee put it, already *"it is hard to find a Fortune 100 company or some facet of our personal lives that has not already been impact materially by cyber... this will just accelerate in the next 10 years."*

"it is hard to find a Fortune 100 company or some facet of our personal lives that has not already been impact materially by cyber..."

Three causes were commonly cited by interviewees as driving the gap between policy and technology:

- **First, there is a human capacity gap where those making policy lack expertise (often technical) to be fully informed on key tradeoff decisions. Unfortunately, the flipside is also true. Academics and others technical experts seldom have the knowhow, ability, and/or desire to engage in policy debates.**
- **Second, while the reach and impact of cyber are incredibly broad, policy making and enforcement institutions are narrow and siloed, making coordinated change more difficult. Unlike other disruptive technologies like telecommunications or the automobile, cyber policy has little chance of being effectively updated or regulated by a single new committee, set of laws, or executive agency.** [4]
- **And third, the pace of innovation is fast and arguably still accelerating, far outstripping the pace with which new policies are made under even the best of circumstances.**

The network is improving, slowly. Some changes may not fully occur until the next gen takes power.

Although there was broad recognition that the network of experts has grown more interconnected and influential over the past 2-3 years as cyber has risen in importance for policymakers as well as the public, large challenges remain including the generational gap between younger digital natives and older digital immigrants. This is particularly true in policymaking, where most senior positions still skew heavily towards those over 50. Several actors noted that *"the perception from several years ago that there was no field blending strategy and cyber is now heavily dated…[because it's now] a field that is clearly taking off."* A common hope is some of the lack of expertise and interdisciplinary thinking the network still exhibits will improve over the next two decades as digital natives rise in the ranks. Opportunities may also exist to empower this new generation within academia, particularly with more digital natives gaining tenure and autonomy in what they study. Surprisingly, these observations were made not just by interviewees under 40, but also by several seasoned experts and policymakers who acknowledged *"a huge generational gap in the quality of cyber experts"* and a *"certain aging off that must occur before we get [fully] to the promised land"* of a more consistent, interdisciplinary network of experts and policymakers.

> *"a huge generational gap in the quality of cyber experts [and a] certain aging off that must occur before we get to the promised land"*

[4] Although a possibility the Initiative will need to plan for under a Trump Administration is a new or consolidated federal agency tasked with owning more of the currently fractured cyber security challenges, as proposed by some influential Republicans like Representative McCaul of Texas.

Politics matter. The network of experts is perceived to lean left while many policymakers and the new Trump Administration lean right.

Political imbalance within the network may be a key driver of experts' lack of trust, connections, and influence with policymakers. The network of experts and many of its key players, including most funded by Hewlett, are perceived as being left-of-center and not having strong connections to and trust from nearly half of DC. Interviews from right-of-center confirmed this concern, noting that even highly successful pieces of research and policy advice like MIT's *"'Key Under Doormats,' barely penetrated into the conservative side"* of policymakers due to the perceived bias of its authors and sponsoring institution. There was also much talk of the influence the 2016 U.S. election could have on the network and its ability to inform policy—clearly reinforced by the subsequent Republican sweep of all branches of U.S. federal government. Anxiety is high given a Trump victory will likely create even more of a gap in government cyber expertise, fueled by a decrease in left-of-center academics, think tanks, advocacy, and media's influence on federal cyber policy, as well as by the replacement of seasoned Executive Branch experts with a host of new political appointees relatively new to government policymaking and cyber. Identifying and engaging the top cyber policymakers in a new Trump administration will be critical if the network wants to continue to expand its ability to inform policymaking.

"'Key Under Doormats,' barely penetrated into the conservative side"

Personal networks have and likely will continue to rule.

Most former policymakers we interviewed lamented the inability of the current network of experts to provide them with informed, unbiased, and policy-savvy advice. They saw most of the experts outside government, with a few exceptions, as either not being experts in what they claimed to be, having a perceived bias that made them untrustworthy, or not understanding policymaking enough for even an informed, unbiased technical opinion to be of much use. Like RTI International's research, we saw that most government policymakers instead relied on personal networks of trusted experts they can quickly and informally consult. Trusted personal networks continue to be the number one way most policymakers get outside expertise. As one highly networked former government policymaker and influential academic put it, *"The trust and network building [I've] seen over the past 8-years was very personal…and [is now] a barrier to a mature network and broader policy influence for those without insider status."* Given *"much of the expertise continues to live in peoples' heads"* not in seldom-read papers, many interviewees pushed for any moves that could *"create a community of people who work on these issues regularly flowing back and forth between government, academic, [and other parts of the network]."*

"much of the expertise continues to live in peoples' heads" not in seldom-read papers

Corporations dominate policy debates, and pursue their own interests.

While the ability of many non-government cyber experts seemed growing but still limited, there was nearly universal consensus that companies already exercised influence through multiple paths, and often crowded out other perspectives. While a few interviewees saw companies as important allies—particularly in the effort to protect individuals' private information from the government—more than half of those who weighed in on this issue saw corporate influence as net negative. This criticism did not simply come from the usual suspects, but from government and corporate insiders as well. Finally, an interviewee now in private industry but with a past in government lamented how he and his corporate colleagues could *"never say what they were really thinking and always had to represent their company's interests first,"* even in situations where their candid expertise would have been far more valuable to the discussion.

> *"[corporate colleagues] could never say what they were really thinking and always had to represent their company's interests first"*

Media and public opinion matter as much as having the "right" technical answer.

Media was often cited as a critical player in the cyber policy debate for its ability to: (i) broadcast to policymakers key events or perspectives, (ii) bolster the public profile of experts and institutions from outside of government, and (iii) build enough public attention or concern about an issue that government or corporate policymakers became more motivated to listen to advice and perspectives from outside their own echo chambers. As one seasoned expert from both advocacy and academia put it, *"the first step [to policy influence] is riling up political opinion and pressure; the second step is having access to and profile with the right people; the last is actually having something to say or propose."* Members of the media themselves confirmed their influence, noting that they were routinely contacted by the White House, Hill, or Executive branch agencies (usually in response to a specific article) asking for either their opinion or connections to a cyber expert who could talk the policymaker through the details. When asked what is the number one area Hewlett may have missed, the most common response was that there was an as of yet undeveloped power the public could have on cyber policy debates as well as policymakers' will to engage experts from outside of government and companies. There are several reasons (e.g. strategy decisions, limited budget, and to a lesser extent issue agnosticism), however, why the Initiative has so far limited its activities to inform and shape the general public's opinion and activism through its grants.

> *"the first step [to policy influence] is riling up political opinion and pressure"*

The network is overly focused on the U.S., and needs to look to the rest of the world.

Finally, interviewees also saw the lack of connectedness between the network of cyber experts and policymakers in the U.S. and the rest of the world as a major impediment. However, from our grantee document review and interviews we found that despite this often-mentioned concern, only a minority of grantees were interacting with international counterparts on any regular basis, and some had almost no interaction at all. As a leading academic with policy experience put it, *"at least for us it's become increasingly clear that we can't make progress on most of the issues we want to impact without a global opportunity."* For a field that already has far more work to be done than resources to do it with, this sets up some challenging tradeoff decisions both for cyber funders and grantees.

> *"it's become increasingly clear that we can't make progress on most of the issues we want to impact without a global opportunity."*

III. WHAT IS WORKING

A key objective of our interviews and document review was to identify which activities and actors are most helping to build the network and/or its ability to inform policy debate/making. Several activities, categories of investment, and specific actors rose to the top, summarized below.

- **Exchanges and fellowships are high return, but a cadre needs to be created for greater impact**
- **More translators and connectors are key to the health and policy influence of the network**
- **The "right" type of convenings have impact, but many are regarded as a waste of time and money**
- **Mapping and informational resources could be transformative, and need to be owned by the network**
- **Mid-sized grants and investments generally rose to the top vs. larger grants**
- **Beyond-grant activities (particularly Hewlett's matchmaking) are well regarded and high return**

Exchanges and fellowships are high return, but more need to occur for real impact.

Exchanges and fellowships were viewed nearly universally as high value and quick to impact. Interviewees believed creating opportunities for exchange of expertise (particularly from outside government in) were effective because they: (i) solved a problem with government not having enough technical expertise, (ii) placed individuals who would normally be outside the circle of trust within it, and (iii) produced lasting personal connections and policy fluency that could be brought back outside of government. Placing relevant expertise and outside perspectives within the belly of the beast also directly combated a reality we heard time and again from former policy makers, that they have almost no time to review written documents, particularly those from outside the government. Consequently, they value personal connections and conversations above all else, both for their expediency as well as for their trustworthiness. As one interviewee with former high level White House cyber experience put it:

"Policy impact is all about getting the right person, in the right place, at the right time. [As a manager of] cyber professionals in the private sector [I] spend most of [my] time recruiting and network building. It should be the same in policy. The number one way to have impact is to put people in the right place. With a marginal dollar to spend, I'd spend it on curated fellowships."

"Policy impact is all about getting the right person, in the right place, at the right time."

Evidence from Hewlett's grants suggests a high return from fellowships as well. Jonathan Mayer, the Stanford graduate student Hewlett has funded for an 18-month fellowship in the enforcement division of the FCC, believes he is having more impact in government than he had before (a profound statement given his career to date). He cites several important benefits of the fellowship, including: (i) new government connections, (ii) a far more developed understanding of how policy is made and influenced, and (iii) lasting credibility with policymakers as someone who understand and values the government perspective. Stanford colleagues as well as other experts saw Jonathan's fellowship as transformative, and as one of the Stanford Cyber Initiative's most important connections to government.

Not everyone, however, agreed that fellowships were the best bet. Pushback on the idea came in two forms: (i) that to be most useful this sort of expertise exchange had to be at least 18 months long and had to happen at scale (i.e. not one-offs), and (ii) that some people believed fellows would simply be coopted by the organizations they were joining. The latter was a less common concern and proponents felt it could be mitigated by carefully choosing fellows and exchange agreement with the hosting organization. The former, however, was a more prominent concern. Multiple interviewees highlighted that individual fellows placed here and there would have limited impact on policymaking writ large. For more measurable change across the network and on policy writ large, multiple interviewees suggested cadre or class of fellows, sustained over time, to fundamentally change both the subject matter expertise of policymakers and the policy savvy and DC connections of an emerging generation of technical experts.

"If you had a tech and privacy person and you imbedded them in every [relevant] committee of Congress, now that would be impactful. You'd normalized [technical expertise in cyber policymaking] and the conversation could instantly elevate."

This approach also matched with a common refrain heard from all but a few interviewees, that it was easier, cheaper, and more effective to make technical types smart on policy than to make policy types smart on technical issues. As one political insider put it:

"I wish rather than trying to make a bunch of poli-sci majors and lawyers savvy on cyber, we took math, CS, and tech majors and made them savvy about policy. You can teach policy quicker than you can teach coding, crypto, or network architecture."

"I wish rather than trying to make a bunch of poli-sci majors and lawyers savvy on cyber, we took math, CS, and tech majors and made them savvy about policy."

The "right" type of convenings have impact, others are "a waste of time and money".

Interviews and grantee documents revealed that convenings are one of the most common activities used to try and connect experts, build trust, and, ultimately inform policy. There was wide variation, however, in both the evidence from grantee documents that convenings were achieving these outcomes as well as whether interviewees saw convenings as a good use of time and money. Interviewees were nearly universally critical of the many convenings they saw as little more than talk shops. Likewise, although there was little grantee reporting to go on given the age of many grants, we saw little claims or evidence that these more ephemeral convenings had lasting impact on the network or its ability to inform policymaking. Several present or past policy makers interviewed suggested they either *"became frustrated very quickly with these events…because they stay very high lev-*

el to the point where they are unhelpful" or because they "too often do not include the key perspectives" needed to make policy decisions. One key influencer went further to say that the formal sessions at most convenings were usually a waste of time and that he and most other savvy influencers *"skip conference content…[but] always go to the meet and greet and the dinners"* because that is where you create personal relationships, connections, and trust. A final skeptic of the proliferation of convenings noted that there are simply too many for all but the well-funded to attend, allowing companies and government agencies with travel budgets to dominate the discussions. To the extent there were proponents for these larger, ephemeral convenings amongst our interviewees, they argued the primary merit of this type of convening was the content they created which could be repackaged and spread more broadly in other media (e.g. podcasts or Twitter).

"became frustrated very quickly with these events… because they stay very high level to the point where they are unhelpful"

What made a good or effective convening was not universally agreed, but several key themes emerged.

- **First, the best convenings focused on trust building, often before information or idea exchange.**
- **They were carefully curated, involved a relatively small number of actors (usually no more than 30), and in many cases were private events closed off to the full network and the broader public.**
- **The convenings cited as most successful were often not one offs, but longer term efforts like the Berklett Group Hewlett funded resulting in the "Don't Panic" report, CSIS commission for the 44th and now 45th Presidents, The Global Commission on Internet Governance, and The Cyber Loop, a members-only online platform for cyber experts.**
- **Additionally, convenings perceived as most effective often had diverse membership, which both made them more effective network building tools as well as provided policy credibility for any recommendations or reports they produced.**
- **Finally, all but the last of these above forums also shared another characteristic, they were convened with the explicit purpose of creating clear, practical policy proposals.**

A leading example of where convenings and policy relevant research overlapped was the Hewlett funded Berklett Group and its publication of the "Don't Panic" report. The Berklett Group stands out as a success for a variety of reasons. First, it was convened by highly credible experts Jonathan Zittrain and Bruce Schneier, who are both leading thinkers and leading influencers with significant public profiles. Second, its membership was diverse and brought experts together that might rarely get the chance to sit and discuss sensitive policy candidly—e.g. experts from academia, think tanks, advocacy groups, private industry, the U.S. national intelligence community, and interestingly, media. Third, the group met regularly, in person, and at length (i.e. for 7-8hrs at a time). And Fourth, from its outset the Berklett group aimed to not just be policy relevant, but to be policy driven and create a product that both could and would be absorbed by policymakers.

Despite the success of Berkman's Berklett Group, its *"Don't Panic"* report, and subsequent media coverage and Hill Testimony, we would note that even this highly effective convening and piece of policy relevant research reportedly had trouble penetrating into the conservative side of the political spectrum and surprisingly still remained unknown to several high-profile interviewees, including former policymakers still active in the field.

For Hewlett, the challenge is how to encourage more of this type of convening, as well as to ensure they reach all sides of the political spectrum. One answer is to sponsor them one at a time, and to encourage others to do the same. The network building impact will, however, be limited and choosing *"winners"* in advance is easier said than done. Another alternative is to look to the fourth example on this list, The Cyber Loop, which was noted independently by seven interviewees as one of the most meaningful network building and information exchanges they participated in. The Cyber Loop is a bit like *"Fight Club,"* in that the first rule seems to be you don't talk much about it. Although members know one another, they do not disclose The Loops full member list to outsiders, and you can only join The Loop if recommended by an existing member and reviewed and approved by a smaller subset of group administrators.

The Cyber Loop is a club, but a highly effective one with a large degree of trust and a diverse membership including, per one members, participants from think tanks, academia, advocacy, industry, the "hacker" community, and multiple past and present policymakers including from the White House. Trust, an interviewee said, *"...is hard to earn, and easy to spend. Before the Cyber Loop, I generally thought trust and networks could only be built in person. But The Loop has shown that is not the case."* The Cyber Loop offers a model the Hewlett Foundation could potentially pursue itself, particularly as at least one interviewee expressed a strong interest in replicating The Loop or something like it for Hewlett grantees, and/or for an international audience to close the many gaps between U.S. experts and their international colleagues.

"I generally thought trust and networks could only be built in person. But The Loop has shown that is not the case."

The importance of translators and connectors.

A common theme across both the push for more fellowships/exchanges as well as for more of the right type of convenings was that for the network to grow and truly inform policy it needs more "translators" and "connectors" [5]—individuals with experience, insights, and credibility in government and/or corporate policy as well as technical issues. Individuals like Danny Weitzner at MIT, Jonathan Zittrain at Harvard, Jennifer Granick at Stanford University, Joe Hall at Center for Democracy and Technology (CDT), Ian Wallace at New America Foundation, Sameer Bhalotra at StackRox, and Angela McKay at Microsoft were cited as examples. These are individuals seen as savvy in both policy and technical issues, and with the type of large professional networks necessary to make new introductions, have trust, and inform policy. As an example, several interviewees noted how one of the

[5] TRANSLATORS: Fluent in both policy-making and technology-making worlds, able to fluidly move between and have influence in both. Bridges divides between the policy and tech "worlds". Encourages an informed and multi-dimensional discussion.

CONNECTORS: Organizers and facilitators of the emerging network. Willing/able to tell you with whom you should be speaking on any issue or topic. Pivotal in passing information/references through the network. Owners and creators of trust and personal capital

key determinates of the relative success of MIT's "Keys Under Doormats" report was Danny Weitzner's familiarity with, and credibility in, the DC policy realm. Similarly, Joe Hall was repeatedly cited as one of the few technologists who truly understood policy, and therefore a frequent translator and connector between experts and policymakers in the network.

Hewlett can arguably increase the number of translators and connectors both by supporting those that are already on that multidisciplinary, policy savvy path, as well as by supporting other actors who do not yet have the right mix of experience and connections but are willing to go and get it, like Stanford technologist and postdoc Jonathan Mayer who is now developing policy experience and connections as a fellow within in the FCC's Enforcement Division. These are also individuals often cited not just as key translators, but also as connectors who were just as likely to connect an interested party with another expert in the network as they were to field that question themselves. Per many, the most important phrase in the emerging network of cyber experts is not *"I can help you"* but rather *"you know who you should really talk to is..."* Master networkers were called out as particularly valuable by former policymakers because they were experts that could be relied on not just for 1:1 advice and translation on short notice, but even more importantly for introductions to a much broader set of experts within his personal network.

> *"[The] most important phrase in the emerging network of cyber experts is not 'I can help you' but rather 'you know who you should really talk to is'"*

A challenge we will discuss in "What's NOT working," is how to make more room for these new translators and connectors when a smaller subset of actors has a first mover advantage, is often dismissive of the need for technical expertise, does not trust those without government experience, and is often willing to opine on cyber questions where other experts are more knowledgeable but not yet known within policy and media circles.

Support for Public Goods: Mapping and Informational Resources

We also saw sporadic but strong support for mapping the field and other informational resources. By far the strongest desire was for a map or list organizing experts by their areas of expertise/research. Experts wanted this to understand what others were working on and with whom they could/should collaborate. Policymakers wanted this list because they do not know who to go to when they have a question, and consequently rely on: (i) known commodities like Jim Lewis, (ii) their own personal networks, or, far less frequently, (iii) new voices cited by knowledgeable media. At least half the policymakers we spoke to said that given the current state of the network, when they needed expertise from outside government their most common course of action was to call a trusted friend and ask them who the top 2-3 experts were on any given issue ~~wh~~o also have a solid understanding of policymaking. As one former government policymaker put it, *"It's all about individual relationships, 1:1s, and personal networks. When I need advice or a connection, I pick up the phone, always."*

> *"It's all about individual relationships... when I need advice or a connection, I pick up the phone, always."*

The challenge is that although many actors know one another at a superficial level, our mapping work, policymaking cases studies, and this evaluation suggest they often are only partially aware of one another's true areas of expertise, interest, and ability. Seven interviewees from across different parts of the network strongly advocated for a network map that would help them and others to not only understand who was in the network, but

who was a leading expert on which issues. As one well-connected, and well-known grantee put it, *"we all know each other [superficially], but aren't talking to one another…I don't really know what others are working on and how, when, or why to collaborate with someone or refer them a question or opportunity."* A different expert with ample government experience noted most policymakers he knew would have loved to have a list of the top five experts and publications in different areas of the field. That said, support for mapping was not universal. A minority of those that weighed in from within the network of experts pushed back on the utility of mapping, noting *"knowing who is who is not one of the problems…the people playing pro-ball all [already] know the other people playing pro-ball."*

> *"we all know each other [superficially], but aren't talking to one another… I don't really know what others are working on and how, when, why to collaborate"*

Although Hewlett has already started to map the field through previous work and this project, developing a more robust answer to these actors' question about who is doing what will ultimately hinge on experts' own willingness to engage with the map and populate it with their detailed profiles and connections. The map we have developed is a starting not an end-point. Improvements could include additional actors, connections, and profile information detailing competency in specific issues (this addition was highly sought after based on our interviews). A more detailed map would either need a substantial investment of additional time from a single actor or a push to crowdsource the relevant information; we would strongly suggest the latter given the Initiative's financial and staff resources, as well as the desire to cultivate a sense of ownership amongst grantees.

Similarly, there was sporadic but at times strong support for the power of other common goods for the field, particularly informational resources like a readily accessible library of relevant cyber policy, legislation, and law, a project already underway at the National Archive with support from Hewlett. It is too early to see if either of these investments will help catalyze the network or, ultimately, its influence on policy, but there were strong voices advocating for both. As a final word of caution, several interviewees expressed skepticism that if the field had not already moved to build an informational resource for themselves Hewlett should not step into do so because sufficient demand did not exist. Several interviewees also noted a high risk that any informational resource created will almost instantaneously be out of date.

Mid-sized grants and investments generally rose to the top.

As the Initiative evolves, one of the trends we believe to be worthy of further exploration is the seemingly quicker turn around and higher production of mid-sized investments. Part of this may be a result of that fact that these grants are also often shorter, and by design produce impact earlier than larger, longer-term investments. Nonetheless, it is interesting to contrast two very different grants to what are otherwise similar organizations. The Harvard Berkman Center convened the Berklett Group and Produced "Don't Panic" with ~$500K, Hewlett has supported three universities with much larger grants of $15M each. It will also be interesting to compare Harvard's relatively lean Berkman Center, Berklett Group, and new Berkman Assembly with Harvard's now far more generously funded ($15M) cyber security program at the Harvard Kennedy School's Belfer Center.

It is not immediately clear that these larger grants will produce more, and some interviewees were highly skeptical of any other institutions' ability to absorb such large donations at this point in the field's infancy. Berkman, New America, and CDT were frequently cited as some of the most effective actors, further supported by our review of their work, yet none were funded at anywhere near the level of Berkeley, MIT, Stanford or, now, the Harvard

Kennedy School's Belfer Center. There is simply not enough evidence in grantee reports to dig deeper into this idea, but it is one we would advocate watching carefully in the future. Our own perspective is that this is less about picking the right or wrong actor as a partner, and more a question of whether anyone was or is ready to absorb and efficiently deploy eight figure grants.

Beyond-grant activities: *matchmaking.*

Finally, multiple grantees and 3rd party experts also had high praise for some of the beyond-grant network building activities of the Cyber Initiative. Most commonly mentioned in a favorable light was Program Officer Eli Sugarman's near constant efforts to connect experts and other actors in the network who he thought should meet or potentially work together. Grantees universally welcomed these connections and introductions, and several called Eli out—despite the confidential nature of the interviews—as a master networker embodying the interdisciplinary, trusted, policy-savvy expert he was trying to create more of. If there was a small point of pushback on this beyond-grant matchmaking, it was that some grantees wanted more information from Hewlett not just on who it thought they should connect with, but why. One grantee also cited the volume of connections, implying Eli was so prolific as a networker that it was in fact hard to follow up on the number of leads he provided, but that they felt obligated to do so. They suggested that rather than stop this value-add beyond grant work, a prioritization of leads and greater clarity on the value Eli saw in each one would be helpful. It is our belief that more deliberate strategy around this matchmaking (e.g., pairing specific academics with specific media or policy savvy members of the network) could be of significant benefit, particularly as several grantees cited both a desire but also difficulty forming partnerships with other Hewlett grantees within the broader network.

IV. WHAT IS NOT WORKING

As one would expect for a new program testing multiple approaches and an evaluation including confidential interviews, there were also several areas where evidence suggests course corrections should be considered. The issues we highlight below include those we determined were most important through our independent review of grantee reporting, as well as those that came up most frequently during grantee and expert interviews. Prominent concerns include that:

- **Academia may not be up to the task of building the network or connecting it to policy debates/making**
- **Policy-relevant research is powerful but quite rare, particularly in academia**
- **Public will and opinion is a largely untapped lever for shifting policy debates and empowering non-government experts**
- **There is not enough "dry power" in the network to react quickly to unforeseen windows of opportunity**
- **Too small a group of high-profile influencers are monopolizing non-government, non-corporate policy influence**
- **The Cyber Initiative's limited funding is spread too thin, and few other funders are materializing fast enough**

There is great variation amongst the anchor grantees both in their approach/strategy to helping build a field/network of experts informing cyber policy, as well as their abilities to deliver on those plans. While it is too early to pass clear judgment on any one of the programs, trends are emerging that warrant a closer look at some anchor grantees activities.

General skepticism from experts interviewed about large grants and academia.

At a high level, there was a large amount of skepticism and sometimes genuine confusion as to why Hewlett had put most its Cyber Initiative budget into three academic institutions, as well as why amongst the many possible academic grantees Berkeley, MIT, and Stanford won out. Quotes, like the ones listed below crystallized into three main concerns, academia's: (i) lack of research into policy-relevant areas, (ii) lack of ability/desire to engage policymakers, the media, and other DC influencers, and (iii) the slow pace of academic research and publications vs. the narrow and sometimes unexpected windows of opportunity to influence policy. These quotes were surprisingly common, with over half of interviewees *(including many academics)* expressing some variation of these concerns. Perhaps most concerning, 100% of the former policymakers we interviewed expressed deep reservations about the utility of most cyber research and writing from academia.

"[The] academic stuff is almost universally not useful. These guys are missing huge swaths of information of how government works and also classified information"

"[The] academic stuff is almost universally not useful. These guys are missing huge swaths of information of how government works and also classified information"

"If [Hewlett is] going to make biggest bets in [academia], they also need to be able to build connections to policymakers. Academia is not always oriented towards policymakers, and often either actively opposed to or afraid of doing so."

"There are structural impediments that discourage serious academics from both true multidisciplinary work and policy influence"

"Academic work and publication often don't penetrate well into formal policymaking in DC or Europe. They don't proactively find ways to come out and shop their research, or make the relationships with Congressional staff to testify or otherwise come out and engage. They're producing work in a vacuum that doesn't often make it out [to DC]"

Although not unique to the field of cyber, another strong criticism of academia came from academics themselves. Several leading scholars and influencers expressed concern that there was no clear path for how to become either expert or influential, other than having past government experience. As a widely respected and influential cyber expert from an anchor grantee put it, *"If you talk to those of us that have 'made it,' the common thread is that there is no common thread. We've all come to it through idiosyncratic paths. When people ask what should I do to [have expertise and influence], I can't answer."* More concerning, this same interviewee noted that if a student asked him if he should attempt to become an expert, he would never recommend it because despite being successful in so many of the ways Hewlett cares about—multidisciplinary, policy-relevant, highly-networked—within academia he was not as successful as some of his more siloed peers; he could not get tenure because there was currently no department where his work and research fit in. Lastly, another leading academic lamented the fact that the field had so far done a poor job of credentialing its experts, creating some sort of clear signal to government and companies about what a cyber savvy lawyer or economists or policy-savvy technologist should look like.

"Academia is not always oriented towards policymakers, and often either actively opposed to or afraid of doing so."

"They're producing work in a vacuum that doesn't often make it out [to DC]"

"If you talk to those of us that have 'made it,' the common thread is that there is no common thread."

Despite some criticism of the three anchor grantees, progress is recognized.

An investigation of the three anchor grantees found that a potential winning strategy towards positive outcomes in field building and policymaking is executing clear plans and activities related to policy-relevant research, media relationships, corporate partnerships, government policy influence, and curriculum development. This aggressive strategy not only bodes well for grantees' work but also aids Hewlett in building a broader network and field that informs, and ultimately, improves policy. While it is important to engage in these activities, grantees should be wary of appearing overly-biased towards corporate relationships and policy in Silicon Valley. Establishing additional contacts and relationships in policymaking hubs could help offset this perception and allow grantees to realize their full potential.

Academic influencers and translators with strong ties to government around national security and encryption are highly regarded within the emerging field, and can help bridge the gap between academia and policymaking. These influencers and translators displayed a strong willingness and ability to partner with actors outside of their institutions to connect to policymaking. MIT's Danny Weitzner, for example, was often cited as one of the leading translators in the field with both past policy experience and enough relevant technical skills. As one interview put it, experts that want to impact the field will line up to work with Danny and MIT because they *"know it's not just going to end up on the pile of policy*

documents."

Overall, all three anchor grantees' work would benefit from focusing on policy-relevant issues, strengthening curriculum development efforts, engaging with outside partners, and leveraging non-academic actors that are key both to network building and to policy connectivity and influence, for example, media, think-tanks, and policymaking actors and institutions.

It is worth noting that no anchor grantee escaped without strong criticism, largely due to a widely held believe amongst almost all non-academic grantees, and in particularly former policymakers, that academic research as currently conceived, incentivized, and executed will rarely shift key policy in either government or the private sector. This poses some larger questions for Hewlett, particularly around if it is playing a long game to slowly build a foundation for new thought and the next generation of cyber experts and policymakers, or if it should seek more expedient and direct paths to informing policy.

Policy relevant research is powerful, but rare.

Similar to convenings, research was a divisive issue that grantee document review and most interviews suggest can build trust and inform policy, but only under the right circumstances. Research is most effective when it is: (i) policy-driven, (ii) backed by a diverse group of authors known to policymakers, (iii) timely, (iv) clearly translates its data and findings into policy implications, and (v) is linked to broader media exposure. As one interviewee from academia who recently got a taste of government work put it, *"the idea that academics will [simply] publish or blog about their work and influence policy is laughable."* Additional interviewees from academia that were nonetheless seasoned informers of policy expressed that *"even policy relevant is too broad. I want our initiative to be addressing problems that are immediately relevant to policy-makers…that are driven by policy."* Although there are certainly examples of this sort of research from within the field and within Hewlett's own Cyber Initiative, this sort of research is rare particularly amongst some of the research being funded through anchor grantee sub-grants.

"the idea that academics will [simply] publish or blog about their work and influence policy is laughable."

As we have discussed previously, two prominent examples of successful policy-relevant research from Hewlett's own portfolio of grants include Berkman's "Don't Panic" and MIT's "Keys Under Doormat." Other examples from Hewlett grantees but not directly sponsored by Hewlett include CSIS' Commission on Cybersecurity for the 44th (and now 45th) President, and R Street's multiple papers breaking down and ultimately supporting the ICANN / IANA transition. In each of these cases, who was saying it was almost as important as what was being said. Berkman and CSIS' work stand out in particular as being well regarded in large part due to the diverse group of experts they assembled, thereby heading off criticism that their report was in some way biased or incomplete. Many of these reports also arrived at the right moment (admittedly sometimes by luck) so they could influence a policy debate live. Lastly, they were written by authors with enough policy savvy that they were not only credible from a technical perspective, but also from a policy perspective where knowledge of past policy debates and actions as well as specific policy recommendations are key.

Much of the research we saw in the field and even much of what Hewlett is supporting (particularly through some anchor grants) appears to lack one or more of the characteristics oft-cited as critical for research informing policy. Even a grantee from one of the organizations we and others deemed more successful at creating policy relevant research noted that *"we publish a ton of stuff, but most of it isn't widely read [in government]".*

"we publish a ton of stuff, but most of it isn't widely read [in government]"

These challenges were by no means unique to academia, although that is perhaps where the gap between research and informing policy is the largest. Under condition of anonymity, multiple think tank and advocacy organizations also conceded their work is often not absorbed by policymakers. *"You have to hit people at the right time with the right product to have real influence"* as one think-tanker put it. *"You can't just put something in the ether and assume it will make it to the right place…research and policy briefs need to be timely, digestible, and rigorous. Often in the think-tank world you get 2 of 3, and that's not enough."*

"You have to hit people at the right time with the right product to have real influence… research and policy briefs need to be timely, digestible, and rigorous."

Even well done research is fighting an uphill battle against two additional major barriers to policy influence: (i) a lasting perception that most of academia is out of touch with policymaking and most of advocacy is biased, and (ii) that even interested decision makers find themselves with almost no time to read papers. As several former policymakers we interviewed expressed, *"the academic stuff is almost universally not useful. These guys are missing huge swaths of information of how government and policy work."* This perspective was not unique; 100% of the former policymakers we talked to expressed deep reservations about the utility of most cyber research and writing from academia. At the same time, these actors were skeptical of academic writing and research, they also noted that even if they weren't skeptical they simply did not have the time to read papers.

"When I was in government, we were all so overwhelmed we just didn't have time to read this stuff. I was working 20 hour days, and maybe reading a few [internal] papers. I had time for whatever was in my inbox, and the crisis of the day. It was all I could do make it through the threat assessments and classified materials. It was the same across government. The director of the FBI is not reading research papers; he couldn't give a shit. And the White House is not reading them either. The signal to noise ratio is way too high. To cut through all this, I had to go back to my old boy network, [to personal connections], and the 20 experts I knew, trusted, and could access quickly."

"The signal to noise ratio is way too high… I had to go back to my old boy network, [to personal connections], and the 20 experts I knew, trusted, and could access quickly."

For research to be more relevant to policy and credible to its decision makers, it needs to:

- **address the issues and challenges policymakers are struggling with as well as how policy is made**
- **have coauthors and partners that lend credibility ~~in~~cluding partisan, political credibility ~~to~~ the work, and**
- **have ties with media or other amplifiers (e.g. think tanks) to get their work in front of non-academic audiences including policymakers.**

The most policy savvy of Hewlett's academic grantees already understand this, and are sometimes working to spread that knowledge to others. In one example, an academic with a background in advocacy brought a high-level policymaker from the Federal Communication Commission to their university so that the policymaker could not only (i) listen to

academics discuss a set of 10 pre-selected issues relevant to the policymake but also so she could (ii) inform academics about the issues she and her team were currently struggling with or considering for the future. This interaction, which cost only an estimated $5K, led not only to new academic-government relationships but also to new, far more policy relevant research.

A key question for Hewlett is the extent to which should continue to let institutions determine their own research agendas vs. if it steps in to point those grantees struggling to make their research relevant towards some of the other grantees (from academia, think tanks, and the advocacy community) that have a stronger sense and track record of creating publications with observable policy impact. Another question is if grantees that are leading experts in their area but lack connections to key amplifiers (e.g., Beltway think tanks, media, and actual policymakers) should receive more direct assistance from Hewlett to close these gaps. One move requested by several grantees is for Hewlett to take an even stronger role in providing media training and connections, so grantee's research and perspectives had a better chance of making it into the mainstream and to reaching influencing public, government, and private sector policy debates.

Not enough "dry powder" to capitalize on unexpected windows of opportunity.

Another common refrain from those trying to inform policy is that the opportunities to do so often come unexpectedly, and are often short-lived. Academics, think tanks, advocacy groups, and other experts need "dry powder" to capitalize on those windows of opportunity (e.g., the ones created by Apple vs. FBI on encryption, by Ted Cruz on ICANN/IANA, by Mandiant on commercial cyber espionage, or by the recent denial of service attacks employing IOT devices). One expert with deep experience in advocacy described how her organization spent nearly 80% of its time focused on creating and exploiting politically opportune moments of influence with governments and/or corporations. Another expert from a prominent think tank described how "Opportunities for influence crop up out of nowhere, and are hard to plan for…[but often] end up being one of the biggest things we did this year." Several grantees lamented that they had to try and make room for this sort of activity from non-grant funds, and that they wished Hewlett either allowed more flexibility in its initial grants and/or had a reserve fund it deployed strategically (and extremely rapidly) on targets of opportunity. An interesting case study from the last three months would be to see how/if Initiative grantees were able to capitalize on the public and government attention briefly focused on the security vulnerability of the IOT as a result of the October 2016 attack taking down multiple high-profile sites across North America.

> *"Opportunities for influence crop up out of nowhere, and are hard to plan for."*

Public attention and will are key, but underinvested in.

A common refrain amongst nearly half of interviewees, further backed by the few network building grantee reports we had, is that one of the driving problems in policy is not only a lack of technical expertise but the fact that even when technical expertise makes it into the room it is often ignored. As a key beltway insider noted, *"a lot of [technical] voices already make it into the debate. But, those voices aren't being listened to and often aren't given the weight they deserve. They are outweighed by politics."* One grantee we and others have identified as effective in informing U.S. government, international, and corporate policy noted how the last thing you need is a good idea.

"The first step [to policy influence] is riling up political opinion and pressure; the second step is having access to and profile with the right people; the last is actually having something solid to say or propose."

"The 1st step [to policy influence] is riling up political opinion and pressure; the 2nd step is having access to and profile with the right people; the last is actually having something solid to say or propose."

Another noted how policymakers were generally all too happy to send some mid or junior level staffer to meet with outside experts, but unless there was political pressure they would be under no obligation to act on their advice. They described meetings with government officials as denial of service attacks perpetrated by policymakers where experts are listened to politely and then nothing changes.

Those within or recently departed from government describe similar exchanges, where they lamented not being able to trust most experts because they were perceived as having one or another bias or agenda. Impartial or at least intellectually honest experts, they felt, were hard to come by. Even academia, which often prides itself on intellectual honesty and neutrality, was seen by many policymakers as inherently biased. Finally, even policymakers admitted that when all the right voices were in the room and the answer was clear, it was often still hard to act due to policymakers' aversion to acting on cyber policy. They noted the political costs of leading a policy change that ended up being perceived as alienating some key constituency (e.g. industry) as far higher than the costs of doing nothing at all.

It would be concerning if while Hewlett and its grantees invest in building a network, policy relevant research, and new connections to policymakers in government and the private sector, their ability to influence (vs. just inform) policy is constrained by a lack of underlying political pressure and support. Many of the grantees that were savvier about influence, particularly the advocacy community and those past government experience, argued for increased investment in educating and/or stimulating the broader populace about cyber issues and risk as part of a larger effort to encourage political and corporate policymakers to seek out and listen to experts from outside their own organizations. Although we saw similar efforts attempted in several of our field-building case studies (e.g. anti-smoking and healthy living), limits to this initiative's budget as well as the breadth and complexity of the cyber field/issues may make this approach harder to apply to cyber.

"Many in the press fear not adequately understanding the foundational issues or the network of experts"

Nonetheless, one idea pushed by several interviewees—and backed up at least in part by network building efforts that have leveraged media exposure as part of their influence strategy—was to fuel this broad public awareness by investing in expanded mainstream media coverage of cyber issues. Several journalists we interviewed that are already well-established leaders in the field of cyber noted that rather than investing in creating one or two more of them, Hewlett or another catalyst should instead invest in a second ring of journalist that do not yet integrate regular coverage of cyber into their work but

could easily do so with some education and incentives. They described *"a pent-up desire amongst peers"* in the White House press corps, national security reporters, business reporters, and others to branch into cyber reporting, but also a *"fear of not adequately understanding the foundational issues or the network of experts"* they would need for story ideas and sources.

This focus on the role public opinion could play in empowering the network of experts and shifting cyber policy for the better also raises the idea of whether Hewlett should remain issue agnostic, or whether its ability to build the network would be amplified if it selected several key debates/issues to. Opinion from interviewees and evidence from grantee reporting was highly mixed on this front, suggesting to us that this is not the moment for Hewlett to abandon its issue agnosticism but that galvanizing the field around 2-3 big tent issues/ideas may be an option to consider once the network is better established.

Too small a group of experts are dominating policy influence.

Another key impediment to network building and informing policy is the concentration of policy influence amongst a small number of individuals perceived as leading cyber experts, often at the expense of other equally or even more qualified experts. These are influencers with outsized public profiles (e.g., as evidenced by the number of times they are cited by policymakers as experts, appear in traditional media, or their social media followings). A second but equally important group of influencers is made up of individuals with former government experience, which we found gives them more access to and credibility with government policy makers. Finally, corporations also have outsized influence due to their economic clout, large number of lobbyists and, more recently in the case of an actor like Google, number of former employees in the White House. The result is that many experts that do not easily fit into one of these categories are often squeezed out of key policy debates. Many of the experts we interviewed noted how the largest, most recognized names in the field were often very willing to brief policymakers on issues they did not have expertise on, rather than expanding and deepening the network by helping connect other actors to those policymakers. *"Too few experts are being asked about everything, including issues they know very little about,"* noted one particularly fed-up interviewee.

> *"Too few experts are being asked about everything, including issues they know very little about"*

This sort of criticism can in part be attributed to sour grapes, but came up frequently enough we feel it is a valid concern Hewlett should at least consider. As one expert put it, if they are not careful *"there's a risk some [Hewlett] grants can actually damage the sector they are trying to nurture. For example, supporting organizations and individuals with more influence than actual expertise."* We agree this is a risk, and suggest Hewlett periodically reconfirm it is striking the right balance between: (i) working through and reinforcing the voices that are already strongest in the field, and (ii) elevating mid-level and/or up and coming influencers to a higher status through new connections, work experience, and/or public exposure (e.g. with media). Our own assessment is that the Initiative is currently striking the correct balance between these levers, in large part due to the investments the Initiative is already making in the next generation through MIT, New America, CSIS, and others grantees.

> *"[Hewlett may be] supporting organizations and individuals with more influence than actual expertise"*

Hewlett non-academic investments may be spread too thin. The desire for a rapid reaction reserve.

A common complaint, some of which we can attribute to jealousy, is that the $15M anchor grants were not the strongest play Hewlett could have made. Behind this concern is a widespread perspective that there is not enough funding in the field to go around. Some experts worry *"Hewlett has spread itself too thin, funding too many org[anization]s and activities"* and that it needs to more quickly *"narrow to the levers and orgs that are highest performing, or they risk losing the progress they've helped make."* Several grantees, including some we saw as particularly effective, expressed they could not continue their work at current scale for much longer because they had not yet been able to find additional funders. *"We're investing a lot of our own money and stealing from other programs to keep cyber afloat at current levels,"* said one grantee. *"We can't keep this up, and will have to roll back our efforts soon if something doesn't change."*

"Hewlett has spread itself too thin, funding too many org[anization]s and activities"

This is difficult territory for Hewlett, as much of its funding is tied up in the three major anchor grants. Although we are cautious that nearly every grantee will identify themselves as high performing, we have nonetheless seen a few actors and activities consistently rising to the top through grantee interviews, interviews with expert 3rd parties, and grantee activities and reporting.

As more grants reach their end and second year annual reporting arrives, we would encourage further consolidation, with some flexible funding held back for network building during the 2017 grant cycle. Our ability to weigh in on other grantees we see rising to the top is severely limited by the young age of most of the grants, and the fact that so few produced even their first, let alone a second or final, grantee report.

V. SUMMARY OF TOP INSIGHTS AND IMPLICATIONS

Insights from this evaluation should influence Initiative decisions on how to further focus its network building grants, staff time, and influence. Summarized below, we have started tying top insights—prioritized by high importance, high feasibility, and low cost[6]—to possible implications for the Initiative moving forward. A summative strategy recommendations memo, to be written by the Cyber Initiative Program Officer with our support, will further prioritize insights and implications from this evaluation as well as our parallel mapping and case studies workstreams.

We would also draw attention to several high-level questions that cut across evaluation insights, and may influence if and how the Initiative responds to each. These include:

How long are you in this effort (5, 10, 20 years), and what risk do you want in your portfolio of investments?

For example, if you plan to wind down in 2 years, it might make sense to refocus discretionary funding on those activities shown to have the clearest and most rapid success, e.g. immediately policy-relevant research, direct exchanges and fellowships, and boutique, highly curated convenings.

What do you see as the right balance between accepting the network as is and maximizing short-term policy impact vs. attempting to fundamentally change the network through longer-term bets?

For example, should you be investing more/fewer dollars in more direct policy influence or increasing investments in identifying, training, and politically empowering the next generation of experts?

Whether the Initiative believes its broad strategy, goal, and outcomes align with its comparatively modest staff and budget—in addition to what it can crowd in from other sources?[7]

If a disconnect exists, either a narrowing of objectives and activities and/or an expansion of Hewlett resources is needed. This decision will strongly influence whether any shifts in the Initiative's network building strategy will be executed primarily through staff time and influence activities and/or through new grants.

[6] **Importance**: How critical is acting on this insight to Outcome 3 success?
Feasibility: How likely is it that Hewlett (or others funders) could rollout the activities needed to capitalize on and/or resolve this insight?
Affordability: How much would it cost to rollout/sustain this response or activity? *(Note: Cost estimates are rough, not fully budgeted projections).*

[7] This evaluation focused on Initiative Outcome 3 (network building). That said, the Initiative may want to focus Outcome 5 (crowing in additional funding) on the activities it believes, in part due to this evaluation, are highest impact. For example, evidence from this report could be used to get additional funders excited about the prospect of expanding the network of expert's political diversity.

CAMBER COLLECTIVE

Operation Environment (1 OF 3)

IMPORTANCE	FEASIBILITY	AFFORDABILITY	EVALUATION INSIGHT	IMPLICATION FOR HEWLETT
●	●	●	**Ingrained Barriers in Government** Barriers within government further increase the gaps between policymaking and cyber expertise. There is a clearly a human capacity gap. Government verticals are not well-suited to developing new policies for cyber, a broad issue with cross-cutting implications.	• Hewlett is already investing in closing the human capital gap in multiple ways and should continue to do so. • It's unclear if Hewlett has any ability to influence more structural barriers, e.g. government verticals and lack of outside access to classified materials.
●	●	●	**Generational Gap** A large generational gap in technical knowledge and interdisciplinary approach exists, with younger digital natives slowly working their way into positions of influence. The trend line is positive, but low; it will be another 20-30 years before things change more naturally.	• Wait for this change to happen or lean in to try and shift the curve. For example, Hewlett could favor investments that accelerate the careers of young, tech-savvy experts vs. working through or further empowering established experts.
●	●	●	**Political Diversity** Is hard to come by in the network of experts, which is perceived as skewing left-of-center. This limits experts and grantees' ability to inform / influence many DC policymakers, particularly on the Hill and in a future Trump-led White House & Executive Branch.	• Hewlett is already aware of the perceived imbalance in the network and amongst its grantees, and is working to combat this. • Particularly given the 2016 election results, it should accelerate this shift and prioritize grants engaging credible, cyber-savvy right-of-center orgs
●	●	●	**Personal Networks** In the absence of a broader network, smaller personal networks rule. Government policymakers rely on who they know personally when they need advice, creating barriers to experts outside government or with no past government experience.	• Accept and try to harness the power of personal networks by developing new ones for key experts through exchanges, targeted convenings, etc. • Complement this system by creating new, or expanding existing, more accessible but still high-trust networks like The Cyber Loop.
●	●	●	**Limited International Network** It is becoming increasingly apparent many cyber policy challenges require international thinking and solutions, yet the network remains highly concentrated in the U.S., with minimal high profile efforts to change this.	• Hewlett will need to continue its expansion into international work, looking for low cost ways to establish new connections. • It could also compel grantees to increase efforts in these areas, either through specific collaboration grants, conditional grants, and/or more beyond-grant matchmaking.

● HIGH
● MEDIUM
● LOW

CAMBER COLLECTIVE

What IS Working (2 OF 3)

IMPORTANCE	FEASIBILITY	AFFORDABILITY	EVALUATION INSIGHT	IMPLICATION FOR HEWLETT
●	●	●	**Exchanges & Fellowships** Shifting experts from one part of the network to another (i.e. academia to gov) is perceived as one of the quickest and most effective ways to build interdisciplinary knowledge, connections, trust, and policy influence.	• Consider expanding efforts in this area to create a cohort of fellows (~20) to effect change on a larger scale and at the same time. • This would require new funding and extensive non-grant negotiation and matchmaking with sponsoring individuals and intuitions. • ID'ing interested sponsors orgs and individuals as well as potential fellows may both became harder, though even more necessary, given Election 2016.
●	●	○	**The Right Convenings** Are powerful tools to build the network and inform policy. Characteristics associated with success include: (i) personal trust building, (ii) careful curation and smaller size, (iii) skillful facilitation, (iv) recurrence, (v) diverse, policy credible members, and (vi) focus on a clear problem / outcome.	• Hewlett could narrow its funding of convenings to only those that do a better job conforming to the best practices emerging from the evaluation. • Alternatively, it could continue funding a variety of convenings but do more to share what is helping the best convenings succeed w/o utilizing the "power of the purse"
●	●	●	**Translators & Connectors** Appear to be particularly important in this nascent field where there is a network-of-networks and large gaps, even animosity, between many government policymakers and non-government experts.	• Hewlett can arguably increase the number of translators by supportingthose that are already on that multidisciplinary, policy savvy path, as well as by encouraging and supporting the next generation of up and comingtranslators and connectors.
●	●	○	**Mid-Sized Grants** And investments generally rose to the top vs. larger grants. E.g. Berkman Klein's Berklett Group convening and "Don't Panic" policy research appeared to do as much to build the network and its ability to inform policymaking as many larger grants.	• Assuming anchor grantee funding is not fungible, Hewlett could nonetheless focus remaining discretionary funds on mid-sized grants, avoiding some of the micro and macro grants that, at least at the time of this evaluation, appear less effective.T
●	●	○	**Top Actors** Are emerging, including amongst Hewlett grantees. For example, amongst academics Berkman (Harvard) and Berkley appear to be leading the way; amongst think tanks New America and CSIS; and amongst advocacy groups CDT.	• Consider focusing discretionary, incremental spend on follow up grants to the smaller handful of grantees with track records already suggesting they are higher performers. • Limit new grantees to those issues where new activities are most needed, e.g. political and international diversity and connections

● HIGH
● MEDIUM
○ LOW

CAMBER COLLECTIVE

IMPORTANCE
FEASIBILITY
AFFORDABILITY

What is NOT Working (3 OF 3)

EVALUATION INSIGHT	IMPLICATION FOR HEWLETT
Academia Is widely regarded by non-academic experts as the wrong place to put the lion's share of Initiative resources. Concerns include: (i) too little focus on policy relevant research, (ii) weak connections to policymaking, and (iii) structural impediments that make inter-disciplinary work and careers difficult.	• Potentially take a more proactive approach with the largest academic grantees, more directly shaping, for example, their: (i) efforts to connect directly with policymakers, (ii) partnerships with others in the network including think tanks and media, (iii) leadership teams, and/or, most controversially (iv) their research agendas.
Research In the network is rarely policy relevant, raising the question of if this is a good way to build network connections and trust or to inform policy debates / making.	• Options for tackling this range from funding certain types of research to helping disconnected experts get a better sense of what policymakers need. • This latter option has been used informally by several academics with good effect, but is not yet systematically employed. • Hewlett could more actively encourage partnerships between orgs with great thinkers /researchers, and those with policy-savvy (e.g. academics and leading think tanks). • Additional, flexible funding could also be made available to help grantees better exploit windows of policy influence created by unexpected events.
Public Opinion Is seen as a major untapped force for network building and policy influence. Experts, particularly those with government or advocacy experience, believe public opinion can push policymakers both to feel a more pressing need to act on cyber, as well as to listen to non-government experts when they do.	• Short-term, Hewlett could help expand cyber media coverage to "2nd ring" actors (e.g. White House press corps, nat'l security and business reporters, etc.). It could also support public "broadcasts" of key cyber events and issues. • Medium-term, Hewlett could soften its issue agnosticism and use more issue-specific research and publications to drive public awareness and pressure for "better" policy.
High Power Influencers "Moguls" A small group of experts with particularly high public profiles may be preventing other experts from rising in the network and/or connecting into policy.	• Hewlett could avoid grants or non-grant activities that further empower these already highly influential actors. • Alternatively, it could focus on: (i) experts that should be part of the policy debate but aren't, and (ii) connectors/translators that possess many of the same character-istics as Moguls but are more likely to share contacts and lift others up with them.
Initiative Resources Until the November budget increase, Initiative resources were insufficient to achieve its broad objectives, and were likely spread too thin to ensure progress and proof of concept in key areas. The annual budget increase helped, but it remains unclear if it will be enough to allow Hewlett to achieve its Outcomes, particularly as funding from other sources has been slow to materialize. As opportunities for informing policy are often hard to predict and short-lived, the Initiative may also be missing opportunities by not having a larger, more flexible strategic reserve it can deploy rapidly.	• As most of the Initiative's budget it already tied up in the 3 anchor grants, every discretionary penny left becomes critical. • Two quick fixes for the disconnect between ambition and resources could be: (i) upping the discretionary spend through an annual budget increase, and (ii) building a reserve to use throughout the year on targets of opportunity. • Finally, Hewlett could shift the terms of its anchor grants to ensure a defined portion of their annual spends go to high priority network building activities, e.g. strategic partners and co-led events outside the universities and outside academia. Grantee efforts to find alternative funding sources have so far produced limited crowding in, indicating further effort in this area is likely necessary.

HIGH
MEDIUM
LOW

INTERVIEW GUIDE

Early evaluation of Cyber Initiative Network building efforts

Dear Participant,

Thank you for taking the time to speak with us. Below please find a short introduction to our work for Hewlett's Cyber Initiative as well as the purpose and content of this interview. Hewlett and Camber want your best and most candid responses, so your comments will be 100% confidential and not linked to either you or your organization. We look forward to speaking with you shortly.

Josh Drake *(Camber Collective)*

I. INTRODUCTION

Camber is connecting with you on behalf of the Hewlett Foundation's Cyber Initiative (CI), as part of a first external evaluation of its work. The project we are leading is focused on Outcome 3 of CI's grant-making strategy—catalyzing a network of experts to build trust and inform more sophisticated cyber policy.

Hewlett's primary objectives for our 6-month project include answering three questions key to successfully catalyze a network of cyber policy experts: (i) What currently exists: Establishing a baseline mapping of the current network of experts, (ii) What is/not working: Assessing the effectiveness of CI's approach to date and potential for impact in the future, and (iii) What next: Recommendations to improve CI's approach and inform sub-strategy development *(i.e. future grant-making)*.

Our project has three main workstreams to inform answers to those questions, including: (i) analyzing field/network building and cyber policy case studies, (ii) creating a map of the network of experts as it exists today –identifying key actors, relationships, paths/barriers to policy input, and (iii) a mid-stream evaluation of the effectiveness of CI's grant and non-grant making activities to date. The last of these, the evaluation, will be based off interviews with grantees and other experts, review of grantee reporting and 3rd party research[8], and insights drawn from field-building and cyber policy cases and network mapping.

The Cyber Initiative has identified you as a key actor for us to talk to as part of our evaluation. For this interview, we would like to ask you a series of questions to capture your insights so *(in combination with other interviews and research)* we can analyze trends and share suggestions with CI and other stakeholders on how to improve their network building activities. If you are a CI grantee, you can assume we have read your most recent grant reporting to Hewlett. In addition to high level questions, we may also have a few specific questions for you about specific elements of your work *(e.g. your efforts to connect with and inform cyber policymakers)*.

DEFINITIONS & TERMS

CYBER POLICY
We take a broad definition of "cyber policy" that includes topics that impact the security, stability, and resilience of a free and open Internet and connected devices. *(Hewlett Foundation, Summer 2016)*

POLICYMAKERS
Members of governments that have a formal and direct role in making, interpreting, or implementing cyber policy *(e.g. members and staff of relevant U.S. Congressional Committees or the Executive Branch and agencies).*

POLICY INFLUENCERS
More broadly, we understand "policy" is also being made by practitioners in field, especially in the private sector *(e.g. those outside government creating norms and processes related to information sharing and coordination for botnet takedowns).*

NETWORK OF EXPERTS
Organizations and individuals working in cyber policy and whose expertise, insights, research, and/or data either is, or should be, an important part of cyber policy debates/making.

TAXONOMIES

CYBER SECTORS
National Security
Individual Rights
Trade/Commerce
Infrastructure

ORGANIZATIONAL TYPES
Government [9]
Academia
Company
Advocacy
Non-Government Body
Philanthropy
Media
"Hacker"
Think Tank
Legal

INFLUENCE TOOLS
Policy Brief
Research Paper
News Article
Conference
Training/education
Social Media
Back-Channel Database
Software
Exchanges/fellowships

[8] E.g. the Cyber Policymaker research conducted by RTI International 2015-2016.

[9] Civilian, Military, Intel

II. CI'S WORKING HYPOTHESES & HIGH-LEVEL EVALUATION QUESTIONS

PLEASE NOTE: Although the below high-level and specific interview questions serve as a preview of the type of conversation we would like to have with you, we hope and expect our actual discussion will be free flowing and dynamic. If we are roughly addressing these key questions and/or what you believe Hewlett most needs to know about its efforts and the network of cyber experts, we are on track. For the interview, we will further tailor both our live and follow up questions to the context of your organization's specific work and experience.

CI's grant making and other efforts in Outcome 3 flows from four central hypotheses about how to catalyze a network:

MAP THE FIELD
A better understanding, shared broadly, about the current network of cyber experts will help all actors understand what is/not working, and how to improve the network's expertise, connectivity, and input into policymaking.

CONVENE DISPARATE ACTORS
Breaking down siloes by creating new opportunities for experts from diverse stakeholder communities to interact/collaborate will increase the quantity/quality of cross silo dialogue, research, rotation, and trust.

CREATE OPPORTUNITIES FOR SHARING EXPERTISE
Exposing cyber experts from one community to educational and/or professional opportunities in another will enable them to learn about each other and give them the tools to communicate, understand each other's view points, and, eventually, collaborate. It will also help build the cohort of much-needed translators.

BUILDING INFORMATIONAL RESOURCES
Informational resources the field can utilize and leverage—for example an online library of key primary documents about cybersecurity policy—will help inform the work of researchers, journalists, civil society, and other members of the nascent cyber policy field.

CI IS MOST INTERESTED IN ANSWERING THE FOLLOWING HIGH-LEVEL QUESTIONS THROUGH THIS EVALUATION

- **Q** Which of CI's activities/approaches are currently working? Where are the early signs of success?
- **Q** Is CI (through its grantees) informing cyber policymaking? What direct/indirect paths are most important?
- **Q** What is NOT working? What is off track, why? What have CI and its grantees tried that has failed, in part or in whole?
- **Q** Is CI missing anything big? Are there areas of network building to inform policy CI is NOT active in, but should be?
- **Q** Has CI made any core assumptions (stated or implied) that we now have reason to question?
- **Q** 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)?

III. DETAILED INTERVIEW QUESTIONS

What's Working? (15 MIN)

PRIMARY

1. What are the 1-3 best examples of success you've seen in building a network of cyber experts informing policy?
2. What do you think has most built trust, developed relationships, and/or increased coordination in the network of cyber experts?
3. What do you think a "better" or higher functioning network of the future should look like?
4. What are the gaps in today's cyber network that would be bridged in tomorrow's? *(i.e. what is currently impeding your or others' ability to partner across the network or bring expertise to bear on policymaking).*
5. Do you agree with CI's 4 primary hypotheses (see box above) for catalyzing a network of experts?
6. Out of these 4 (and any you added in your response to Q1-2), which are you most pursuing and/or do you believe are most important?

SECONDARY

- Do you share CI's strong focus on network building as key to building trust and improving policymaking, or do you see some other potential lever as mattering even more *(e.g. policy-relevant research)?*
- Is there any element of either CI's push to be more multi-disciplinary or more connected to policy that you are having trouble with? What are the impediments you would like to see removed?
- Has CI missed any network-building activities you see as key?
- Are CI's activities, in your view, plugging the top gaps you laid out in Q4?

III. DETAILED INTERVIEW QUESTIONS CONTINUED

How is Policy being Informed? (15 MIN)

PRIMARY

7 What have you seen most leading to policy influence across and by the network of cyber experts?

8 What specific types of tools have you seen as most effective in informing policymakers (see list on page 1 for a potential list of "tools")?

9 Who do you see as primary translators between key groups in the network? What makes them so? Who they know, what they know, or how they say it?

SECONDARY

- What indicators/evidence do you see of your orgs's access to and ability to inform policymakers?
- Where do you see the highest value (returns vs. effort) investments to experts better informing policy making?
- What relationships, with peers, policymakers, or others seem to be most important?
- Who do you see outside of formal policymakers (i.e. govt) having the most influence on policy debate?

What's Not Working? What Is CI Missing? (15 MIN)

PRIMARY

10 In your own work, is there anything you have tried or were hoping to achieve that is either slow to materialize or just not working out?

11 Do you see CI trying anything that you think has notably missed the mark, or is substantively less impactful than ready alternatives?

12 Do you see any major assumptions on the part of CI that you think need to be revisited? *(Please consider assumptions that are part of the network building hypotheses on page 2 as well as other assumptions CI may not yet be fully aware it is making).*

SECONDARY

- What is the top example of something you are struggling with vis-à-vis connecting with other parts of the network or having policy impact?
- Has/is CI doing anything you think violates "do no harm" *(i.e. inadvertently damaging the network, policy debates, or policymaking)*?
- E.g. The importance of Hewlett and CI remaining "issue agnostic".

Other Questions (10 MIN)

PRIMARY

13 If you were to know now that CI would not extend beyond its current 5-year, Board-approved duration, would you advise changing anything about its grant making and/or non-grant activities?

14 Is there anything else about the network of cyber experts and policy impact that I have not asked about but should know?

15 Lastly, do you have any questions for Camber about either this evaluation, or the field/network building case study and mapping sections of this project?

SECONDARY

- NA
- NA
- NA