WILLIAM + FLORA
Hewlett
Foundation

Cyber Initiative

NOVEMBER 2017

GOAL

To cultivate a field comprised of institutions with deep expertise to which decision-makers can turn, and in which they and the public can place justified confidence, for solutions to pressing cyber policy challenges.

I. INTRODUCTION

Cyber threats are growing like Topsy, and we lack the institutions, ideas, and teams of experts needed to anticipate and address them. It is difficult to overstate the seriousness of the situation. We are still in the very early stages, yet cybersecurity breaches are already causing huge economic harm. Worse, they are eroding trust in the computer systems and infrastructure on which our government, our businesses, and our daily lives depend. The risks reach everything from voting to registering for school, protecting the nation, managing the electric grid, enforcing criminal law, providing access to healthcare, purchasing a mortgage, and paying bills or buying groceries. We cannot continue managing these risks as we have: frantically putting fires out as they appear, never knowing for sure when or where the next one is coming—or in what form. We need established institutions with independence and depth of expertise to anticipate, analyze, and address the risks thoughtfully and systematically.

The Hewlett Foundation launched the Cyber Initiative in March 2014, with the goal of building a capable field of cyber policy experts and expertise.[1] By year three, we had concluded that it would probably make sense to ask the board for a five-year renewal upon expiration of the initial five-year term, which would be next year. But the 2016 election dramatically raised awareness about cybersecurity—highlighting new needs, but also creating new opportunities. Among other things, concern for protecting election infrastructure and democratic institutions has generated widespread interest that offers significant new opportunities for field-building—opportunities the Hewlett Foundation is uniquely positioned to seize by virtue of our cross-sectional expertise from the combination of the Cyber and Madison Initiatives.

[1] We define "cyber policy" broadly to include not only traditional notions of computer and information security, but also the full range of related policy issues, such as Internet governance, net neutrality, encryption, surveillance, and privacy.

We believe it important to begin capitalizing on these developments now given the importance of the moment in which we find ourselves. But it is difficult to do so in the fourth year of a five-year effort. The foundation cannot responsibly initiate new efforts that may take more than a year to bring to fruition without some assurance that it will be able to follow through. The problem is still more acute for grantees, who are justifiably reluctant to launch new efforts and commit resources and staffing with only a 12-month runway. For that reason, the Hewlett Foundation's board approved a five-year extension of the Cyber Initiative a year early, meaning the effort will run through 2023.

For the same reasons, the board approved a modest budget increase to $10 million per year beginning in 2018 (i.e., our 2018 budget will increase from $8 million to $10 million and then remain at that level until 2023). These funds will allow us to continue current efforts while pursuing new opportunities to build the field through efforts to protect U.S. elections and democratic infrastructure from cyber-attacks.

It is, simultaneously, a timely moment to revise our strategy, given the results of a recently completed external evaluation (which supported what we were already learning from experience and from input from the board and others). Our work to date attempted to do too many things at once, not all of which were essential, but all of which did help us learn. The revised strategy thus simplifies our approach and focuses our funding—concentrating on a smaller number of core tasks, while eliminating or scaling back more peripheral efforts. Put briefly, to build a durable and enduring cyber policy field, we need to do the following three things going forward:

(i) Build a set of core institutions with sufficient depth of expertise to deliver solutions that take competing values and trade-offs to pressing cyber-policy challenges seriously.

(ii) Create a talent pipeline to produce experts with the necessary mix of technical and non-technical skills and knowledge to staff these and other institutions, including government and industry.

(iii) Support the development of infrastructure to translate and disseminate the work of these institutions into forms that can be understood and used by decision-makers and the public.

We have already made significant progress in each of these areas, though an additional push is needed to achieve the "escape velocity" needed for the field to become self-sustaining. Building a robust cybersecurity policy field is a daunting task whose difficulty should not be underestimated. But the circumstances are ripe to succeed—an ironic but nevertheless fortuitous outcome of the election and other high-profile cybersecurity breaches of the past year.

We will know we have succeeded when, as cybersecurity problems arise and evolve, there exist institutions to which decision-makers can turn in which they and the public may place justified confidence.

II. THE CYBERSECURITY CHALLENGE

Few people would have identified cybersecurity as a major social problem when we began investigating it in 2012. Outside the tech community, most people thought of it as an inconvenience at most—annoying spam and silly requests from "Nigerian strangers" seeking help to acquire fortunes. We were almost alone in insisting that cyber threats posed a looming threat to our economy, society, and government, and that we needed to get ahead of the problem.

A lot has happened since then. Much more quickly than even we anticipated, cybersecurity has become the master problem of the Information Age—evidenced by its now regular appearance on the front pages. Today, anyone can advertise, buy, bank, argue, steal, and even fight wars in cyberspace. Yet digital technologies have been introduced with little consideration of their immediate and long-term ramifications. Increasing reliance on artificial intelligence and networked machines poses unanticipated risks both to the workforce and to national security. High-profile cyber threats extend far beyond mere data breaches to include hacks of the power grid, holding hospitals ransom, and more.

Meanwhile, laws, norms, and policies—not to mention the decision-makers who shape them[2]—are struggling, and failing, to keep up. Yet unlike other complex and multifaceted domains, such as public health or nuclear security, there exists no cohesive body of institutions with the necessary cyber policy expertise to respond to pressing challenges.

Government and industry spend vast amounts to build cyber weapons and firewalls to punish or foil bad actors. But it's not enough to combat cyber threats directly. We need to mitigate cyber threats, as we have other threats, by developing and adopting appropriate norms, policies, and practices to anticipate and head off potential dangers. Equally important, we need sophisticated, independent analysis to think through the difficult tradeoffs that new technologies inescapably pose. This is where we and our grantees come in.

Below, we offer three concrete examples of our grantees' work. The examples are illustrative of the kinds of concerns the cyber field touches and the types of solutions our grantees have produced. We deliberately shied away from choosing the most urgent or frightening cyber threats. Instead, we chose archetypes to demonstrate in a less loaded manner how building a more capable cyber policy field will benefit society.

Encryption. Complaining that terrorists and criminals use encryption to hide their malicious activities, officials in law enforcement have tried to compel technology companies to decrypt data relevant to their investigations. Their concerns seem valid, but so do the fears of critics in civil society and industry, who worry that mandated decryption will weaken online safety and security and hurt U.S. commerce.

This long-simmering debate began to mature in July 2015, following the release of an influential report—funded by the Cyber Initiative—prepared at MIT by a diverse group of leading experts. "*Keys Under Doormats*" persuasively explained how government efforts to access encrypted communications at scale are technically infeasible and dangerous. These conclusions were then bolstered by a second report, prepared by a different group of Hewlett-funded experts under the auspices of Harvard's Berkman-Klein Center. "*Don't Panic: Making Progress on the Going Dark Debate*" argued that encryption was not in fact causing law enforcement to go dark; the report has been downloaded more than 100,000 times from Harvard's website.

It is critical to get this issue right: unnecessary or badly designed encryption regulations will significantly affect the Internet, and not for the better. The debate is not yet over, but our grantees at MIT and Harvard played a crucial role by developing sophisticated arguments based on careful analysis of the evidence and policy tradeoffs. Their work helped put the debate on firmer ground, staving off a short-sighted and potentially dangerous policy decision that would undermine cybersecurity online.

International Cyber Norms. Cyberspace is often described as the new "Wild West" because it lacks clear laws or norms to control the wide array of malicious actors who are active there. Efforts to establish norms that limit different kinds of harmful conduct in cyberspace have not been wanting—whether through the United Nations or by individual governments or private companies. Lacking adequate expertise or credibility, or both, these efforts have all fallen flat.

The Cyber Initiative played a critical role persuading experts at the Carnegie Endowment for International Peace (CEIP) to pay attention to cybersecurity. CEIP focused on the most strategically destabilizing cyber attacks: attacks of a kind that all governments could presumably agree should be eschewed in all circumstances. Capitalizing on contacts and credibility developed over years from work in other areas, CEIP began a campaign of quiet conversations with key states and companies to develop the content of potential norms.

[2] Decision-makers include not only federal, state, and local policymakers, but also the companies that develop, own and operate key Internet infrastructure, whose terms of service govern individual Internet user's conduct online.

CEIP focused its initial efforts on protecting the integrity of financial data, because the complex, interdependent nature of the international financial system makes every nation that participates vulnerable in the event of an attack. CEIP received positive feedback from major banks, insurers, and government representatives (including Russia and China, which, like the U.S., must rely on this system), and their proposed norm was included in the March 2017 Communiqué of the G20 Finance Ministers and Central Bank Governors. It's a critical first step in establishing clear rules that protect the international finance system and its constitutive banks and customers.

Driverless Cars. The number of driverless cars in use is expected to grow very quickly over the next two decades, with upwards of 30 million partially or fully autonomous cars being sold annually by 2035.[3] In an attempt proactively to address the likely societal impacts of this trend, the National Highway Transportation Safety Administration issued guidelines in late 2016 for the testing and deployment of autonomous vehicles. These guidelines, which are voluntary, do little to address serious security concerns associated with the millions of lines of software code in a modern car.

Media reports notwithstanding, it will be some time until driverless cars become commonly available and used. In the meantime, we have provided support to a number of grantees, including R Street and the Tech Policy Lab, to get ahead of the many thorny security challenges associated with automated vehicles. This includes efforts to: (i) increase the number of experts properly trained to solve these specific security problems; (ii) make sure that cyber security solutions don't overlook or undermine other concerns, like conventional car safety or privacy; (iii) ensure that technical "solutions" take into account what we know about human behavior; and, (iv) identify the most serious problems, as well as problems that may have been overlooked.

We are proud of the work described in these examples (and could provide many more), but we offer these mainly to show concretely how important it is to build this field and how critical a role the Hewlett Foundation is playing in helping to do so.

III. THE FUNDING LANDSCAPE AND POTENTIAL FOR PHILANTHROPY

One reason our role is critical is that we were the first funder in this space, and we are still the largest one. A number of large foundations have begun making grants, mostly for open Internet and human rights-focused advocacy and research. A few other funders have begun to dedicate resources to exploring the national security dimensions of cybersecurity. With steady efforts and hard work, we have made progress in increasing both the number of funders and the size of their grants. New foundations, such as the Bradley Foundation and Charles Koch Institute, have begun grantmaking, and key academic grantees, such as the Belfer Center at Harvard, have succeeded in attracting significant new support for their cybersecurity activities.

Sadly, the Internet entrepreneurs who made their fortunes creating the technologies that give rise to cybersecurity problems have shown no inclination to help address them. They are missing in action—as is government, which has focused its resources on technical training while putting next to nothing into policy work. Companies, meanwhile, are understandably animated by commercial imperatives and short-term profits: private sector funding, unsurprisingly, tends to focus on developing new products and defending corporate networks. The upshot is that cybersecurity is a classic arena for philanthropy, a problem for which charitable resources are uniquely necessary.

[3] See e.g. https://www.bcg.com/industries/automotive/autonomous-vehicle-adoption-study.aspx.

IV. REVISING OUR STRATEGY

The urgency of the cyber problem is clear. As noted in our opening paragraph, we live in a world that depends utterly on computers and the Internet. We must be able to trust these systems or everything comes apart. But threats to that trust are not static, and there is no single or permanent answer to them. We must, rather, find ways to anticipate and manage an evolving set of challenges. And for that we need a system of institutions with the necessary intellectual, human, and financial resources to earn, and warrant, our confidence.

But how to build such a system? The Cyber Initiative's original vision benefited from a flexible design that facilitated learning and adaptation in its initial years. In early 2017, we received the results of our first external evaluation. Drawing upon more than 40 hours of confidential interviews with more than 30 experts (including grantees, industry experts, and former policymakers), the evaluation confirmed the importance of the Initiative and found that we are on a promising path. While concluding that many of our grants are having their intended impact, the evaluators nevertheless recommended adjustments.

Most important, and consistent with our own informal assessment, the evaluation advised us to simplify the strategy and focus our funding on a smaller number of projects. Our initial approach of spreading resources among a wide range of efforts and organizations was crucial for learning, but it stretched us too thin. We are now ready to concentrate our funds among fewer grantees in the service of a distilled set of outcomes.

The Initiative's original goal of building a strong, sustainable field of cyber policy is unchanged, but to achieve that goal we need to narrow our focus to three things: (i) building a set of core institutions with sufficient depth of expertise to deliver solutions that take competing values and trade-offs to pressing cyber-policy challenges seriously; (ii) creating a talent pipeline that produces experts with the necessary mix of technical and non-technical skills and knowledge to staff these and other institutions, including government and industry; and, (iii) supporting the development of infrastructure to translate and disseminate the work of these institutions into forms that can be used by decisionmakers and understood by the public.

We have made progress in all three areas. We touch on this briefly below, but focus primarily on where we need to go from here.

A. BUILDING CORE INSTITUTIONS

The first of the priorities enumerated above—building institutions to which decision-makers can turn and in which they and the public can place justified confidence—will likely absorb the bulk of our grant dollars going forward. This was already a focus, of course, and we have supported a number of universities, think-tanks, and policy centers to produce high quality research and analysis.

We have, however, been funding too many organizations, typically awarding modest project support in the form of one-year grants of $100,000-$300,000. This made sense in the early learning stage. But while it may have produced some strong work, it is insufficient to enable these organizations to develop the depth and expertise needed for strong, sustainable programs. It is also too little for them to recruit and underwrite the next generation of scholars and analysts.

We plan to remedy this going forward by providing greater support to a smaller number of organizations. Experience in other fields suggests that a modest number of strong institutions is sufficient to engender a productive network, which then prompts other organizations to join in. This has already been our experience in the academic space, where our catalytic grants to MIT, Berkeley, and Stanford have prompted other universities to establish programs of their own.

Going forward, in other words, we will build a cadre of anchor institutions in the policy development space by making larger, longer, and more flexible grants to a smaller number of grantees—no more than five or six. These anchor grantees may take different organizational forms, though think-tanks and policy-oriented academic centers are the most likely candidates.

In supporting—or, if need be, building—organizations, we are looking to equip them with three critical attributes:

- First, intellectual resources that bridge technical and policy domains. This requires staff from different backgrounds with different skillsets who share a collaborative mindset. Technologists, lawyers, economists, national security practitioners, and experts from other disciplines must work together, shoulder-to-shoulder, to effectively tackle cybersecurity policy problems. Not every organization must incorporate every discipline, of course, but they must favor a multidisciplinary approach and hire a sufficiently deep bench of talent. We also expect teams to be cross-generational, grooming a next generation of experts who can build on the work of existing leaders in the nascent field.

- Second, sensitivity to the inescapable tradeoffs that must be made among security, privacy, civil liberties, and commerce. The field is not helped by—and we will not fund —institutions that deny or fail to treat seriously genuine tensions that cyber policy poses among core democratic values (like those exhibited in the examples discussed in Part II). Nor will we fund groups whose work indicates precommitment to an already known "right" answer, particularly if empirically unsupported or badly supported. Grantees can, of course, have an institutional viewpoint: they can be liberal or conservative or libertarian or whatever. We will, in fact, consciously seek to support institutions with different viewpoints, in the hope of generating a diverse array of policy options for decision-makers. But the organizations we support must have a demonstrated commitment to open-minded, empirical investigation, including honest consideration of opposing views and of the costs and benefits associated with different policy options.

  Achieving this kind of balance has never been easy, and it is harder than ever in today's politically and intellectually polarized environment. It's also more important—a fact driven home daily by the degradation of policy debate and dearth of good policy solutions we get from institutions that begin with their conclusions and try to promote them by shouting more loudly and more frequently than "the other guy." Cyber debates have so far escaped this kind of polarization, and part of our goal must be to keep it that way.

- Third, credibility among the key stakeholders and communities—left and right; technology and policy; East Coast, West Coast, and middle; U.S. and international. Realistically, we are unlikely to find organizations that are trusted by all parties on all sides. Given today's tribal politics, any organization, no matter how good its work, is likely to be perceived as biased by at least some constituencies. While striving to support organizations with broad credibility, then, we will be looking to assemble a portfolio of grantees that, collectively, cover all the necessary bases.[4]

[4] Our recent evaluation found that, while we fund a range of centrist, progressive, and right-of-center groups, our overall grantee pool leans (and is perceived to lean) to the left. This is so even though cybersecurity is still less partisan or politicized than most issues. Diversifying our family of grantees by prioritizing the addition of right-of-center groups and/or increasing support to those we already fund is thus wise, particularly given the U.S. cyber policy outlook of the next few years.

In addition to these three characteristics, we want the anchor institutions we support also to become adept at both fundraising and strategic communications—essential functions if they want to leverage their expertise and disseminate their ideas and work product. This includes investing in non-cyber policy staff, and in other functions needed to operate a high-quality organization. We can and will help grantees do this by providing general operating support and, where appropriate, organizational effectiveness grants. But to grow and thrive over time, they will need to raise funds beyond ours and engage external partners, including key decisionmakers.

Institutions that satisfy these conditions are presently in short supply. Most organizations have at most one or two people, usually with little experience or diversity of background, and often with rigid ideologies. Our evaluation found that two of the Initiative's three anchor university grantees are clearly on a path to achieve the necessary expertise and credibility; Stanford has lagged, but we are optimistic that a recent change in leadership has put it on the right track.

A few of the think tanks and other centers we have supported are likewise well positioned to grow and excel with appropriate support. We might also consider launching new institutions if we find gaps that cannot be filled by strengthening existing organizations. As noted above, the number of institutions needed to generate a robust field can be relatively small if these institutions are sufficiently strong and broad. Other funders agree and have expressed willingness to consider funding new groups.

B. BUILDING A TALENT PIPELINE

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

We are well along the way to achieving this goal. Our anchor university grantees have all begun or will soon launch interdisciplinary degree programs or concentrations in cyber policy. MIT added an Internet policy track to its Master's degree in Science, Technology, and Society (STS), and it has already placed a number of students in leading tech companies, the U.S. government, and several international organizations. Berkeley and Stanford will launch similar programs in 2018—Berkeley in the form of a new Master's degree in cybersecurity, Stanford as a new cyber policy track within its International Policy Studies Master's Degree.

As we hoped, other universities have taken steps to catch up. To name only a few, NYU has introduced a new Master's Degree in Cybersecurity Risk and Strategy, the University of Washington has started offering courses through its interdisciplinary Tech Policy Lab, and the University of Texas at Austin will begin offering a cybersecurity certificate program. The number of universities offering interdisciplinary cyber policy courses or degrees has grown large enough that Stanford has organized a conference (with Hewlett funding) at which participants can share curriculum design, course materials, and lessons learned.

We expect to provide continued support to sustain and increase this momentum, though we will likely begin to condition our support on matching funds. We intend also to seek out some new academic institutions to provide greater geographic diversity and to ensure we are serving diverse student populations.

The long-term viability of these educational efforts depend on nurturing continued faculty interest. At present, teaching in a multidisciplinary cyber program is a post-tenure luxury. There is no shortage of teachers, but we need to know there will be a next generation. One way to nudge the process is to create a cohort of Hewlett Foundation Cyber Scholars, selected via a competitive process, to teach and pursue policy research.

c. TRANSLATION INFRASTRUCTURE

While focusing most of our efforts on institution building, we will continue to dedicate a portion of our resources to enlarging the field's capacity to translate and disseminate ideas to decisionmakers and the public. Achieving this goal requires four interrelated efforts on our part: (1) training individuals to translate and explain ideas and bridge stakeholder communities; (2) helping organizations convene diverse stakeholders and develop capacity to communicate their ideas; (3) building independent platforms to distribute new research and ideas; and (4) developing narrative devices (frameworks, metaphors, images, and stories) that are useful for communicating ideas to non-expert audiences. We briefly discuss each of these in turn.

(1) Our recent evaluation highlighted the importance of "translators": individuals who can work across sectors (government, academia, industry) to communicate ideas and facilitate cross-sector collaboration. Fellowships and exchange programs have proved effective for this purpose, and we are currently exploring a number of new fellowship grants, building on a very successful grant that placed a cybersecurity fellow from Stanford at the FCC. We have also retained communications experts to train individual translators about how to communicate strategically.

(2) Similar modest investments in training can have significant and immediate impact on our grantees' institutional communications capacity—teaching them how to make their policy ideas more accessible and how to develop productive relationships with policymakers and media. Over time, we expect our larger grantees to bring this capacity in-house by hiring dedicated communications staff.

Another way we improve our grantees' institutional communications capacity is by fostering or supporting partnerships between media-savvy grantees and grantees who lack the capacity or resources to manage communications on their own. We are also funding organizations to convene diverse groups of stakeholders, such as the Berkman-Klein effort mentioned above and the new Aspen Institute Cyber Strategy Group. Efforts like these are quite inexpensive, especially relative to their potential impact.

Another inexpensive but highly productive way to improve translation and communication is by supporting cyber policy trainings or "boot camps" for journalists, Hollywood writers and producers, policymakers, and other key audiences. Grantees spend a few days with a group—teaching concepts and vocabulary, providing a framework to guide their understanding, and getting them excited about the issues. Several grantees have developed curricula for these sessions, and we may host one ourselves in 2018—bringing leading journalists together with experts from our network with the twin goals of positioning our grantees as trusted sources while improving the quality of journalism.

(3) A well developed field needs independent outlets to translate, disseminate, and distribute new ideas and important developments. Traditionally, this was the function of printed journals. But while these still play a role, people increasingly turn to blogs and Internet-based platforms for information. We support a number of such platforms and will continue to do so. The best example may be Lawfare, a widely read and respected blog we helped grow (whose readership increased 1100% this past year). Lawfare is unique in the way it effectively amplifies the ideas of both leading and emerging experts in the field while actively soliciting divergent viewpoints to feature.

Cyber policy is a new field, and the media landscape is still developing. We are actively exploring whether to create new media platforms and/or other channels to help cyber experts translate, disseminate, and make available their policy ideas.

(4) Non-expert audiences, not to mention ordinary citizens, need narrative aids (e.g., metaphors, accessible framing devices, graphic representations) to understand the complex, technical issues that inform cyber policy. We have already funded the Carnegie Endowment to develop a series of analogies to explain cybersecurity concepts to senior military and national security officials who lack a background in the field. A project we are currently examining—one requested by grantees—is whether to fund the creation of openly licensed imagery (photographs, infographics, graphic art, etc.) that could be used without charge to depict and demystify cyber concepts.

D. INTERNATIONAL GRANTMAKING

Our international grants to date, mainly in India and Germany, are having real impact. But they also confirm our intuition that Hewlett cannot by itself build a global network of strong cyber policy institutions. Yet because solutions to many cyber policy problems must be both globally accepted and applied, we will continue looking for opportunities to make international grants that strengthen field capacity overall. Being realistic, we do not expect grants for this purpose to exceed 10-15 percent of the Initiative's annual grant budget.

We support institutions outside the U.S. to ensure the development and introduction of different perspectives on critical problems. We will continue looking for projects that can catalyze the maturation of cyber policy thinking in other countries, particularly if they are able to attract matching in-country funding. We will also begin to press our U.S. grantees to develop partnerships and collaborative relationships with counterparts outside the U.S. One way to facilitate such relationships could be to convene domestic and international grantees and other organizations on issues of shared interest—such as, for example, what to do about cyberattacks against democratic institutions and infrastructure.

V. WHAT SUCCESS LOOKS LIKE & HOW WE'LL MEASURE IT

How will we will know if or when we have succeeded?

- First, we will have established a set of core institutions that meet the criteria described above: strong staff with an appropriate mix of technical and non-technical expertise, high quality work that wrestles with complicated trade-offs; and credibility with decisionmakers and decisionmakers who are called upon to solve pressing cyber policy challenges.

- Second, interdisciplinary educational programs will exist to train cyber policy experts and help place them in key roles within industry, government, civil society, and academia.

- Third, there will be specialized journals, blogs, and other media platforms to make cyber policy ideas and solutions accessible and intelligible to decisionmakers.

We expect interest in the field to continue growing among funders, evidenced by grants and other support to the institutions we help build. We will continue our outreach efforts, but the best way to attract money into the field is to build organizations capable of doing important work and able to fundraise for themselves.

We have developed a rigorous monitoring plan with implementation markers for each of the three strategic priorities discussed above. We will collect data on an ongoing basis from four main sources: (i) annual grantee reports; (ii) an annual survey of 30 external, non-grantee cyber experts; (iii) data collected by the Cyber Initiative team on a semi-annual basis; and, (iv) research compiled by a third party evaluator.