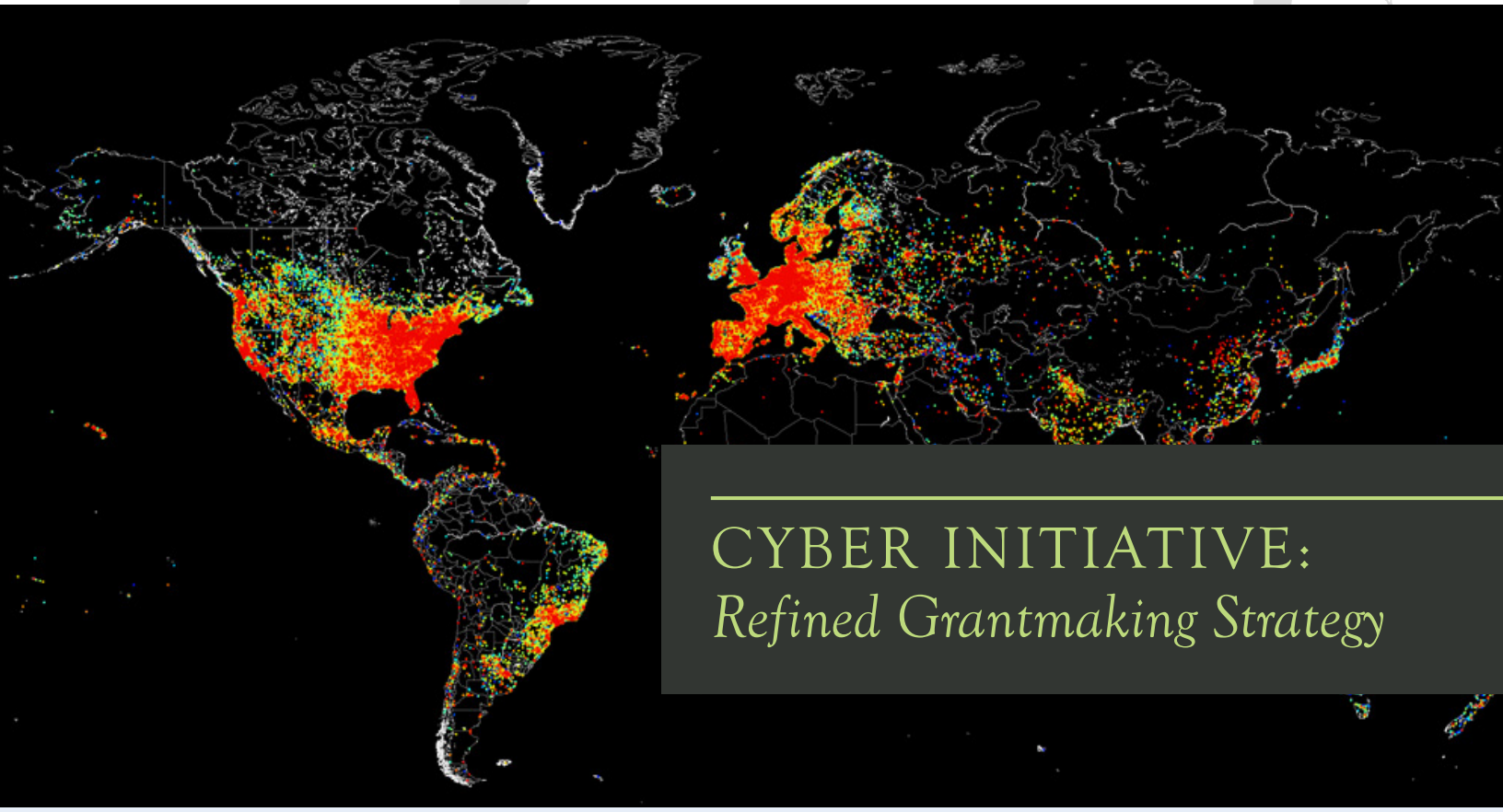


CYBER INITIATIVE:
Refined Grantmaking Strategy

THE WILLIAM AND FLORA HEWLETT FOUNDATION

MARCH 2016

CYBER INITIATIVE: *Refined Grantmaking Strategy*

MARCH 2016

The William and Flora Hewlett Foundation helps people build measurably better lives, concentrating its resources on activities in education, the environment, global development and population, performing arts, and philanthropy, as well as grants to support disadvantaged communities in the San Francisco Bay Area.

The Hewlett Foundation's Cyber Initiative makes grants to help support the development of a robust, multidisciplinary cybersecurity field that serves the public interest.

On the web: ***www.hewlett.org***

(Cover Image) **A heat-map of every internet-connected device.**
IMAGE : *John Matherly, Shodan.io* USED WITH PERMISSION

REFINING OUR GRANTMAKING STRATEGY

The Hewlett Foundation launched the Cyber Initiative in March of 2014. 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. This way, we capture not only more 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 are a neutral player who—unlike government or industry—is not perceived as motivated by profit, politics, or self-interest. We are, moreover, explicitly agnostic as to specific policy outcomes, seeking only to generate better, more robust debate and analysis around medium- and long-term cyber policies and strategies, and to stimulate the development of new policy frameworks that address the tensions and tradeoffs between different values (civil liberties, innovation, national security, etc.) and contribute to making better strategic policy decisions.

The Hewlett Foundation Board awarded the Initiative $20 million to be expended over a five-year period ending in 2019. This was supplemented in November 2014 with an additional $45 million for three large grants. Given this and the arrival of a new program officer, we decided to take early stock of our progress. Informed by lessons learned over the past eighteen months, this document describes our plans for moving forward with a modestly refined goal and strategy for advancing it.

The problem we're focused on has not materially changed since the Initiative's launch, but our early grants have deepened our understanding of the problem's key drivers and helped us hone our approach to addressing them. They have also validated our focus on field building to inform better policymaking.

Panelists for the plenary session "Public-Private Collaboration on Cybersecurity": (left to right) Elizabeth Sherwood-Randall, Bernard Tyson, Mark McLaughlin, Anthony Early Jr, Kenneth Chenault, and moderator Jeh Johnson.

PHOTO : *L.A. Cicero*

The Cyber Initiative has been well received by key stakeholders in government, the private sector, academia, civil society, and philanthropy. We have made two sets of grants so far: large institutional grants of $15 million each to UC Berkeley, MIT, and Stanford; and, more targeted grants to individual think tanks, civil society groups, and academic centers. The former funded the creation of new cyber policy centers on each campus to educate students in a multidisciplinary fashion and pursue new policy-relevant research. The latter focus on specific policy challenges, outputs, and/or individual elements of the strategy described below.

Together, our grantees are beginning to build the foundations of a more sophisticated field.

As elaborated below, this early experience has led us to refine the Initiative's goal, encapsulating it in a clearer statement of purpose—which is, namely, to cultivate a field that develops thoughtful, multidisciplinary solutions to complex cyber policy challenges, and by this means catalyzes better policy outcomes. We'll seek to achieve this purpose by making grants focused around five core objectives:

- **BUILDING THE CAPACITY OF CIVIL SOCIETY ORGANIZATIONS**
- **BUILDING THE CAPACITY OF DECISION-MAKERS AND INFLUENCERS**
- **BUILDING A ROBUST NETWORK OF EXPERTS**
- **GENERATING POLICY DRIVEN RESEARCH AND THOUGHT LEADERSHIP**
- **CATALYZING ADDITIONAL FUNDING**

We explain these objectives in greater below, including examples of current and likely future grantmaking within each.

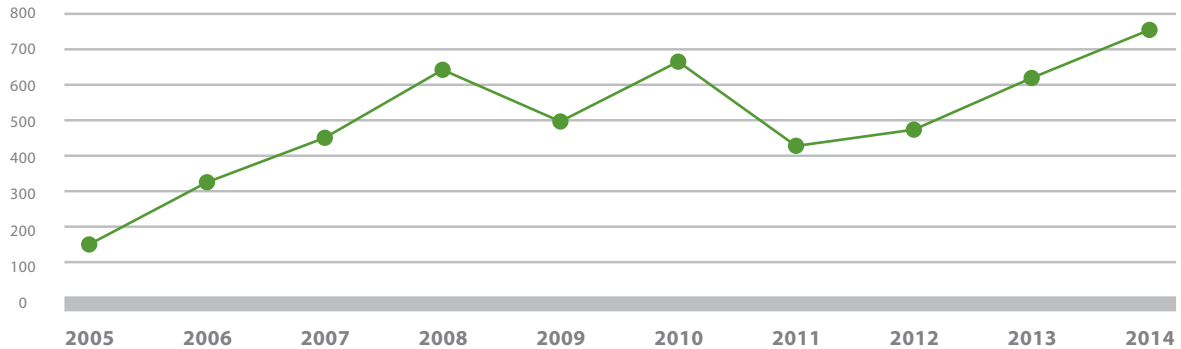
Building a robust cybersecurity policy field is a daunting task whose difficulty should not be underestimated. The Cyber Initiative can play an important role, but will not succeed by itself. We are seeking to play the role of catalyst, leading the way by showing what can be done while encouraging other funders, including government and industry, to widen their focus. Our remaining grants budget of $4-5 million per year allows us to continue seeding the field and enticing others, but is not by itself adequate to achieve our goals. We plan to leverage the Foundation's reputation, experience to date, quality of grantees, and ongoing investments—along with increasing public attention to and awareness of the importance of cybersecurity—to attract other large funders. At some point in the future, however, if a somewhat larger investment could make a difference, we may also ask the Board to consider allocating additional resources.

THE PROBLEM AND WHY IT MATTERS

High profile breaches in both the public and private sectors—at Sony Pictures, Anthem, and the Office of Personnel Management, among many others—underscore the magnitude and importance of the problem the Cyber Initiative seeks to address, as well as the centrality of its charitable purpose.

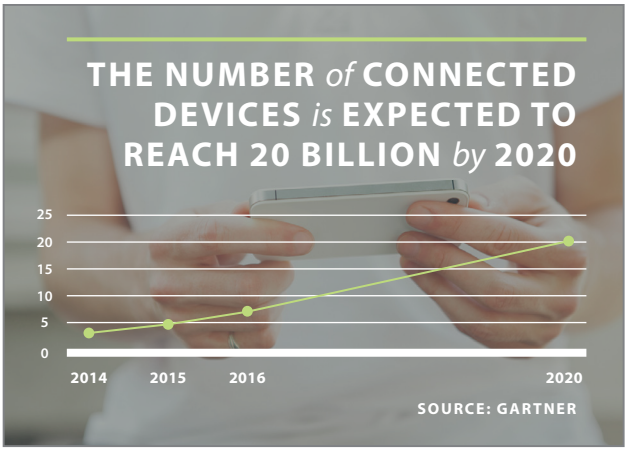
Policymakers are struggling to make informed and sophisticated decisions about cybersecurity policy matters in part because long-trusted Industrial Age norms and laws may be ill-suited for an information era. They freely admit they do not fully understand the complexity of the issues, which makes it well-nigh impossible to focus on the right problems; properly balance competing values, such as national security and civil liberties; or grasp the long-term impacts or tradeoffs embodied in their decisions. In crucial respects the field is, frankly, still embryonic: too underdeveloped to provide the information, policy frameworks, venues for dialogue, and leadership required to drive more balanced policy decisions and strategies.[1]

THE NUMBER *of* REPORTED DATA BREACHES *has* INCREASED MORE THAN 4X *in* THE LAST 10 YEARS



SOURCE: ID THEFT CENTER

[1] For a concrete example of how the U.S. government is struggling to respond to the OPM breach with little support from the policy research community, see e.g. *http://www.nytimes.com/2015/08/01/world/asia/us-decides-to-retaliate-against-chinas-hacking.html?hp&action=click&pgtype=Homepage&module=first-column-region&region=top-news&WT.nav=top-news&_r=0.*



In the meantime, global Internet traffic continues its explosive growth, as does the number of Internet-connected devices and sensors (the "Internet of Things"). Digital technologies promise greater access to information, increased efficiency and economic growth, opportunities for creativity and expression, and new forms of social interaction. The growth in Internet use, along with society's increasing reliance on networked information technology to assist in decision making or perform automated functions, can also have unanticipated risks. There can be a variety of unintended, often negative, societal implications associated with new technologies and complex systems that do not emerge immediately, but rather are time-delayed.

Yet people need to be able to count on the digital tools of their everyday lives even though every new Internet user and/or device is another potential prospect for malicious actors to exploit. They need trustworthy devices and systems that function as expected. Disruptions to such trustworthiness—whether due to the purposeful actions of an adversary or an unexpected, emergent property of a complex system—could give rise to serious threats to national security, commerce, and individuals alike. The decisions policymakers and societies make about how to manage these risks, moreover, will likely have enormous consequences for privacy and civil liberties, economic organization, and international relations in the future.

As the original strategy paper described in greater detail, five interrelated factors drive this problem:

1. There is a dearth of civil society organizations that take a multidisciplinary—as opposed to purely technical or non-technical approach—to the cyber policy debate.

2. There exist far too few well-rounded experts—fully conversant in both the technical and non-technical aspects of cybersecurity—to translate between the policy and technical communities and help make better policy decisions.

3. There is no network or global community of cyber policy experts. The field is fragmented between multiple communities, each with its own culture, vocabulary, and agendas.

4. There is a shortage of high-quality policy research, analysis, and thought leadership.

5. Limited resources are available to address the policy dimensions of cybersecurity. Nearly all government and corporate spending focuses on technical responses to cybersecurity only or narrow agendas. And other funders are reticent to start new grantmaking.

OUR GOAL

The goal of the Cyber Initiative is to cultivate a field that develops thoughtful, multidisciplinary solutions to complex cyber policy challenges and catalyzes better policy outcomes.

We seek to reach that goal by achieving five outcomes that correspond directly to the five problem drivers articulated above. These are: (1) to build civil society organizations that take a holistic, multidisciplinary approach to cybersecurity and contribute to a more informed policy debate; (2) to educate and expand the knowledge base of existing decision-makers, and educate and empower an emerging generation of cyber policy experts; (3) to foster the emergence of a network—comprised of experts from industry, government, think tanks, academia, and elsewhere—that builds trust and promotes collaboration; (4) to fund new policy driven research and thought leadership by experts from diverse professional, political, and intellectual perspectives; and (5) to catalyze additional funding on cyber policy topics from philanthropic, government, and private sector sources.

GRANTMAKING TO DATE

As we hoped, the three universities we selected to receive large institutional grants last year—both individually and through collaboration—are playing an important cross-cutting role. These three $15 million grants have produced noteworthy ripple effects by serving as anchors for the budding field and for our field-building efforts. In addition to generating policy-relevant research and educating emerging cyber policy leaders, each university has begun to convene key stakeholders, initiate new dialogues, and collaborate with other Cyber Initiative grantees. Their leadership and stature will be invaluable as we assemble a diverse portfolio of smaller, non-university grantees. The chart below highlights just a few of the universities' activities to date:

STANFORD

- *Broad focus on Cyber Social Systems -- the interaction between cyber technologies and existing human social systems.*
- *Co-hosted the Presidential Summit on Cybersecurity and Consumer Protection in February 2015.*
- *Twelve initial grants made to Stanford researchers in July 2015.*

MIT

- *Launched the MIT Cybersecurity and Internet Policy Initiative.*
- *Coordinated an experts' report on encryption that was covered on the front page of the NY Times in July 2015.*
- *Joint cyber policy class bringing together MIT engineers with Georgetown law students is underway.*

UC BERKELEY

- *Launched Center for Long-Term Cybersecurity (CLTC).*
- *Hired former Pentagon cyber policy official as inaugural fellow.*
- *Held two-day scenario planning exercise to focus work of CLTC.*
- *Developing new multidisciplinary Master's Degree in Cybersecurity.*

Our other grants—mainly to think tanks and research outfits, but also to some other universities—have complemented the work of Berkeley, MIT, and Stanford. These are typically modest in size, ranging from $100,000 to $400,000 per year. And unlike the broad university grants, which were designed to cover all aspects of the Initiative, they focus on individual goals and specific policy questions. Rather than recount each grant in detail, we depict their chief features in the chart below, which offers a portrait of the Initiative to date:

CYBER INITIATIVE GRANTS MADE *as of* NOVEMBER 30, 2015

SIZE *of* GRANT *per year*	ORGANIZATION	OUTCOME 1 *Civil Society*	OUTCOME 2 *Decision Makers*	OUTCOME 3 *Network*	OUTCOME 4 *Policy Research*	OUTCOME 5 *Funding*
LESS THAN $100,000	ATLANTIC COUNCIL	●	●			
	NYU		○	●	○	●
$100,000 TO $249,999	GEORGE WASHINGTON UNIVERSITY		○	●	●	●
	TAXPAYERS FOR COMMON SENSE		●		●	
	NATIONAL SECURITY ARCHIVE	●	●	○	●	
	CENTER FOR DEMOCRACY *and* TECHNOLOGY	○		●	●	
	IDEAS42		○		●	
	CARNEGIE MELLON	●	●	●	○	
	STANFORD		●	○	○	●
	WILSON CENTER		●	○		
$250,000 TO $500,000	NYU		●	●	●	
	NATIONAL ACADEMIES *of* SCIENCES		●	●	●	●
	PUBLIC KNOWLEDGE	●	○	○	●	
	TECH POLICY LAB	○	●	●	●	
	VIRGINIA TECH		●	●	○	
	CARNEGIE ENDOWMENT	○	●	○	●	●
	RAND		●	○	●	
	CENTER *for a* NEW AMERICAN SECURITY	●		○	●	
	BERKMAN CENTER	○	○	●	●	
	NEW VENTURE FUND			●	●	
	NEW AMERICA	●	●	●	●	

● PRIMARY EMPHASIS ○ SECONDARY EMPHASIS

MOVING FORWARD

1. BUILDING THE CAPACITY OF CIVIL SOCIETY ORGANIZATIONS

Build civil society organizations that take a holistic, multidisciplinary approach to cybersecurity and contribute to a more informed policy debate.

Technologists, lawyers, economists, national security practitioners, and experts from other disciplines must work together, shoulder-to-shoulder, to effectively tackle cybersecurity policy problems. Unfortunately, with rare exceptions, think-tanks, advocacy organizations, universities, and other civil society groups have yet to adopt such an approach. Very few civil society groups have technologists (computer scientists, engineers, etc.) in senior policy positions, which limits their understanding of cybersecurity and contributes to the technology versus policy cultural divide. Even fewer organizations are home to former intelligence community, military, and/or law enforcement practitioners with deep national security experience. This starves civil society of critical insights, not to mention how to communicate effectively with influential government stakeholders (who oftentimes are the most resistant to policy change).

The Cyber Initiative is exploring opportunities to help encourage national security practitioners to join civil society organizations and supports organizations that seek to hire such individuals. We will also endeavor to create a pipeline of former military and military intelligence veterans interested in civil society cyber policy efforts. One of our earliest grants thus funded New America to become the first U.S. think-tank that brings technology, law/policy, and national expertise to bear on cybersecurity policy issues.

Congressional staff members attend the second Congressional Cyber Boot Camp at Stanford University in August 2015.
PHOTO : *Rod Searcey*

Likewise, few universities embrace a multidisciplinary approach to cyber research and education. Our grants to Berkeley, MIT, and Stanford established a core of influential universities to set a strong example. We will wait to make large grants to other universities until results of existing university grants become clearer, but will explore complementary efforts in the meantime. We will also seek geographic diversity in our future university grantees to ensure maximum impact.

Another challenge is that, at present, almost all prominent civil society groups are clustered on the liberal side of the ideological spectrum. This imbalance must be corrected to encourage new thinking, but also to connect with and influence moderate and conservative individuals and officials. We are exploring opportunities to support greater ideological diversity within civil society and advocacy organizations. New groups may need to be created if existing groups prove unable or unwilling to take a multidisciplinary and ideologically balanced approach on cyber issues. Other funders and experts in the field agree with this view and have expressed willingness to consider funding new groups and emerging voices in the field.

2. BUILDING THE CAPACITY OF INDIVIDUAL DECISION-MAKERS AND INFLUENCERS

Educate and expand the knowledge base of existing decision-makers, and educate and empower an emerging generation of cyber policy experts and influencers.

The need for individual capacity building is acute in underserved parts of the executive branch (that is, in most civilian agencies), and among members of Congress, their staff, federal and state judges, state and local government officials, and key non-governmental influencers, such as journalists. Our efforts will likely focus on one or more of these critical, yet severely under-resourced, groups. Other foundations, such as the MacArthur Foundation, are focused on assisting underserved parts of the executive branch, which may provide an opportunity for collaboration.

We plan to work with universities and civil society groups to develop and deploy nonpartisan cyber policy education and training programs for these core constituencies. Stanford's Congressional Cyber Boot Camp—a three-day immersive training for senior Hill staff—is a good example of the type of targeted, substantive effort we will seek to replicate.[2] Programs can be tailored to the groups' needs and provide a balanced, technical and policy primer in the key issues relevant to each group. We will encourage communities to learn from each other and to reflect upon which materials and training approaches are most effective. Over time, the trainings will become more advanced to reflect the groups' increasing knowledge base.

We also seek to build an emerging generation of experts with both technical and non-technical skills to understand the multiple facets of cybersecurity and serve as translators on the issues. Our university grantees are core to this effort and will be complemented by additional academic grantees to broaden the effort. We want not only to educate future experts but also to help see that they are placed in influential positions within key stakeholder communities.

[2] For additional details on the program, please see: *http://www.hoover.org/events/congressional-cyber-boot-camp-2015*.

3. BUILDING A ROBUST NETWORK OF CYBERSECURITY EXPERTS

Support the emergence of a network–comprised of experts from industry, government, think tanks, academia, and elsewhere–that builds trust and promotes collaboration.

This is a daunting task given the fragmented, siloed nature of the field. At present, multiple chasms separate the technology and policy communities, researchers and vendors, and civil society and government, to name only a few. Each group uses its own vocabulary and has its own culture. There are few translators who are trusted by multiple stakeholder groups and can effectively communicate among them.

Participants discuss "A Cybersecurity Policy Research Agenda for the Internet of Things" during a meeting at the Hewlett Foundation in April 2015.
PHOTO : *Kate Payne, Hewlett Foundation*

We are planning four activities to address these challenges: (a) mapping the field; (b) providing opportunities for different stakeholders to convene together; (c) exposing experts from one community to professional opportunities in others; and (d) building informational resources that the field can leverage. Several existing grantees, including the Berkman Center and New America, have already launched network-building efforts to further these objectives.

MAPPING THE FIELD. We continue to scope the field and gather key data points. Looking forward, we will focus particularly on obstacles to field cohesion, such as the chilling of certain types of cybersecurity research due to regulatory and legal restrictions. We will also continue to map key stakeholder opinions (using tools like the government policymaker survey described below).

OPPORTUNITIES FOR JOINT CONVENINGS. We will try to break down siloes by creating new opportunities and fora in which experts from diverse stakeholder communities can interact and collaborate. Existing fora—including leading conferences and academic meetings—typically cater to a single community and do little to promote collaboration across siloes or cross-pollination of ideas. Here, we will experiment with different formats, beginning with smaller-scale, curated gatherings to ensure a positive group dynamic and then attempting to scale the most successful models. For example, we are funding the Berkman Center to bring together academics, civil society, and senior national security leadership, and enable them to openly share their views, learn from one another, and identify new policy solutions.

OPPORTUNITIES FOR SHARING EXPERTISE. We will also expose cyber experts from one community to educational and/or professional opportunities in another, through such things as boot camps, internships, fellowships, and exchanges. We will fund opportunities for technologists to develop policy experience and expertise and for policy experts to deepen their knowledge of technology. This will enable different cybersecurity expert communities 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 us build the cohort of much-needed translators.

BUILDING INFORMATIONAL RESOURCES. We will continue to fund informational resources that the field can utilize and leverage. We have funded the National Security Archive to create an open online library of key primary documents about cybersecurity policy, and we made a grant to Taxpayers for Common Sense to create a database of U.S. government spending on cybersecurity. These will provide invaluable resources for researchers, journalists, civil society, and other members of the nascent cyber policy field.

4. GENERATING POLICY DRIVEN RESEARCH AND THOUGHT LEADERSHIP

Better inform policymakers by funding new policy driven[3] research and writing by thought leaders from diverse professional, political, and intellectual perspectives.

Multiple grantees, including RAND, the Carnegie Endowment, and New America, are already generating new policy ideas and infusing them into the public and policymaker discourse. We will continue to work with Stanford, UC Berkeley, and MIT to ensure that their various strands of cyber research have policy relevance and are not redundant and/or overly academic. In July 2015, MIT coordinated a study entitled "Keys Under Doormats," co-authored by several leading cryptologists, that explains the technical challenges of giving the government plain-text access to otherwise encrypted communications. It is a good example of what is possible because its release was timed to coincide with Congressional hearings on the topic and was featured in the New York Times.[4]


The New York Times http://nyti.ms/1H739kz

TECHNOLOGY

Security Experts Oppose Government Access to Encrypted Communication

By NICOLE PERLROTH JULY 7, 2015

SAN FRANCISCO — An elite group of security technologists has concluded that the American and British governments cannot demand special access to encrypted communications without putting the world's most confidential data and critical infrastructure in danger.

A new paper from the group, made up of 14 of the world's pre-eminent cryptographers and computer scientists, is a formidable salvo in a skirmish between intelligence and law enforcement leaders, and technologists and privacy advocates. After Edward J. Snowden's revelations — with security breaches and awareness of nation-state surveillance at a record high and data moving online at breakneck speeds — encryption has emerged as a major issue in the debate over privacy rights.

That has put Silicon Valley at the center of a tug of war. Technology companies including Apple, Microsoft and Google have been moving to encrypt more of their corporate and customer data after learning that the National Security Agency and its counterparts were siphoning off digital

Going forward, we will fund groups with the capacity to produce sophisticated and innovative multidisciplinary research on cyber policy topics. Topics may range from data gathering and analysis to empowering evidence-based decision making to analytical frameworks that shape long-term government strategy and doctrine. Two particularly promising areas of further study are (1) the relationship between trustworthiness problems and geostrategic security, including how to build a safer Internet infrastructure and how to limit the risks of and/or damage caused by international cyber conflict; and (2) the likelihood of emergent, unintended properties of cyberspace with unexpected consequences for people and society.

[3] We support research that is consciously driven by a desire to inform policy debates, requires interaction with policymakers, and addresses concrete policy questions (whether current or future). We do not support research that is policy relevant only to the extent that it could conceivably impact a policymaker's thinking at some point in the future.

[4] See e.g. http://www.nytimes.com/2015/07/08/technology/code-specialists-oppose-us-and-british-government-access-to-encrypted-communication.html?ref=topics&_r=0

We will look to our three university grantees to help lead this effort by weaving together the multidisciplinary strands required to create a new discipline (building on their experience developing a new nuclear security discipline over previous decades). But we certainly remain open to other organizations and entities to play key roles.

To help ensure that we're meeting the needs and interests of our primary audience—policymakers—we're holding ongoing conversations with experts in the field, as well as with government decision makers. We have contracted with Research Triangle International to survey government cyber policymakers to gain a more in-depth understanding of the research they prioritize and how best to deliver it. This knowledge will build upon our initial insights gained during the original scoping of the Initiative and subsequent conversations with government. We expect the survey to help us, our grantees, and other funders better understand the policy landscape and where our activities will have the most impact or face the most resistance.

While our focus is on generating policy that looks ahead, policymakers also need help on the issues they are wrestling with right now. We must remain nimble enough to take advantage of select targets of opportunity to inform current and near-term policy discussion—especially as what we learn from our work makes some of these policy issues ripe for action. We need, in other words, to be responsive to policymaker demand as policymakers become aware of and interested in the Cyber Initiative. An example is our grant to George Washington University to convene a working group to study "active defense"—an issue attracting increasing attention in Washington, DC—from a balanced perspective, which we hope will generate a framework to inform better future decision making.

5. CATALYZING ADDITIONAL FUNDING

Catalyze additional funding from philanthropic, government, and private sector sources on cyber policy topics.

We have started to demonstrate with our early grants that philanthropy can play a useful role in cyber policy, and we have used some of these grants to attract new funders into the field—partnering with them to give them the full benefit of our work, allay their concerns, share risk, and build their knowledge. To date, we have co-funded grants with the MacArthur Foundation, the Carnegie Corporation, the Sloan Foundation, and the Smith Richardson Foundation. We have also partnered with leading technology companies like Google in jointly funded projects.

It's a start, but more needs to be done—much more. Attracting additional funders and additional resources into the effort is critical for a strong field to emerge. We will, therefore, need to give this outcome more attention going forward. We will start by surveying the funding community in greater detail—partly to gain a more granular understanding of other funders who are funding in the areas of technology and cyber policy, but also to identify new potential funders (e.g. legacy security funders, new Silicon Valley-based funders, corporate foundations affiliated with breeched companies, and the like). Based on this research and our experience to date, we might also commission a study to identify various areas of need that could be of interest to funders with particular ideological or substantive perspectives. For example, the majority of foundations that currently fund in this area employ a civil liberties, human rights, or social justice lens. Their approaches likely would not appeal to more national security-minded foundations, which are just starting to express an interest in cybersecurity. We will work with grantees and potential grantees to find appropriate funders, highlighting what they do and thereby providing additional concrete examples of worthwhile funding opportunities.

We will also engage in thoughtful, concerted public outreach—including everything from blogging, and public speaking to presentations at philanthropic events and roundtables. We will deploy Hewlett Foundation staff, including its president and Cyber Initiative program officer (as well as willing Board members) to hold face-to-face meetings with other foundations to encourage them to enter this new funding space. We may also convene other foundations and potential funders for a day long workshop and training on cybersecurity and cyber policy issues, which will offer potential grantees an opportunity to explain what they do and why it matters.

We are presently exploring ways to engage the U.S. government, especially the White House, in calling upon philanthropy to step up and begin working on cyber policy, explaining that there are important things that need to be done that government cannot do and industry will not do. We will continue our discussions with the U.S. Department of State, NSA, DHS, and National Science Foundation about potential opportunities for collaboration. We are also in touch with the EU about how best to encourage U.S. and European academics and think-tanks to work together on cyber policy analysis and research.

We will likewise seek out opportunities to encourage foreign funders to enter the cyber funding space, and we are pursuing partnerships with leading European foundations.

RISKS

The risks articulated in the original *March 2014 strategy paper* largely remain relevant today. First, changes in technology are constantly reshaping the nature of the threats and potential for solutions, as well as giving rise to new problems. Second, we must engage a diverse array of groups with whom we are still building relationships—ranging from start-up owners to hackers—yet whose buy-in is critical. Third, industry and government may not want independent research about cybersecurity. Fourth, cyber experts in different sectors may have little interest in interacting with each other. Fifth, organizations we fund may not be capable of bridging the gap between key stakeholders. Sixth and last, other funders may prove uninterested or unwilling to enter the cybersecurity field.

Based on our efforts over the past year and a half, we believe that most of these risks can be overcome, but it will take time and commitment, including both human and financial resources. Initial responses to the Cyber Initiative have been very positive across the board—whether from industry, civil society, independent security researchers, or other key members of the field. The United States government, EU, and other governments have been unexpectedly supportive and are actually supplying ideas for policy research; industry, too, seems eager to collaborate, and a number of important companies have already co-funded projects with us. We are working hard to manage grantee expectations by emphasizing the importance of diversifying funding sources—and helping grantees engage with other funders—so they do not become overly dependent on our funding.

However, overcoming the field's deep chasms and lack of trust is difficult. We believe there is sufficient interest and understanding from key individuals in all the stakeholder communities, breaking down the siloes and building connective tissue among different expert communities is and will remain the Initiative's central challenge.

Eliciting new funding has also proven difficult and time-consuming. We have demonstrated modest initial progress, but expectations should be kept in check. We do not anticipate a huge infusion of new support arising from our efforts right away, but these early signs combined with increasing public awareness give us confidence that we will succeed if we are patient and work hard. As explained above, we plan to make fundraising a priority and will deploy a multifaceted engagement strategy to unlock new sources of funding. The ultimate success of the Initiative will turn in large part on our ability to complement our own funding with significant funding from other foundations, government, industry, and individual philanthropists.

MONITORING AND EVALUATION

TRACKING PROGRESS. We are tracking general indicators of progress in the form of "directional" outcomes (meaning increased amounts of specified outputs, like research, collaborations, funding, and the like), but we cannot yet provide quantifiable, specific targets. This is to be expected given the difficulty in measuring the progress of a field-building strategy and the fact that we're just eighteen months in. We hope to articulate more specific targets over time, as a baseline develops and we learn more from our efforts.

As noted above, we are nevertheless tracking directional outcomes through the use of implementation markers—things inside or outside the strategy's sphere of influence that serve as useful proxies to indicate whether we're making progress or need to consider course corrections. We have defined nine such markers that we are beginning to track across our five outcomes, as shown in the chart below.

We are also thinking about the role and use of external advisors, either informal or formal. We will give additional thought to the creation of a standing advisory group and/or use of more informal or ad hoc advisors. They will also be helpful as we refine our efforts to track progress.

CYBER INITIATIVE: DIRECTIONAL OUTCOMES & IMPLEMENTATION MARKERS

BUILDING CAPACITY *of* CIVIL SOCIETY ORGANIZATIONS	1. *Civil society groups begin to hire technologists, national security practitioners, and other relevant experts.* 2. *Civil society demonstrates increased ideological diversity among, including expansion of centrist organizations.*
BUILDING CAPACITY *of* DECISION-MAKERS	3. *Policymakers participate in capacity building activities.* 4. *Graduates of educational programs receive increased job offerings.* 5. *A larger number of universities begin to implement a multidisciplinary approach to education.*
BUILDING A NETWORK *of* EXPERTS	6. *New gatherings of cyber policy experts from technical, non-technical, and other key stakeholder communities are launched.*
GENERATING POLICY DRIVEN RESEARCH	7. *Credible and policy-relevant research is produced by civil society groups.* 8. *New ideas contained in thought leadership are actively discussed at the policy level.*
CATALYZING ADDITIONAL FUNDING	9. *Current and new funders express interest in funding new work on cyber policy.*

Evaluating the work. We will work on an ongoing basis with an outside evaluator to assess our efforts so we can adjust our strategy in real time, as needed. We have begun an initial evaluation focusing on our third outcome (building a network of experts). We believe this outcome provides the greatest opportunity for learning, because it is likely the hardest to achieve in the short term. Potential evaluation questions include: have cyber experts in industry, government, academia, and other relevant sectors begun working together? If so, what are the key enablers? If not, why not? Are there particular forces that can promote or inhibit the emergence of a network? Subsequent evaluations in 2016 will focus on whether and to what degree we're making progress on our other outcomes.

PRIORITIES FOR 2016

In the coming year, the Cyber Initiative will begin to ramp up activity on many fronts. In addition to work on fundraising, which we discussed above, three specific priorities for 2016 are:

EXPLORATORY INTERNATIONAL GRANTS. We want to begin exploring potential grants to non-U.S. based grantees. This is a change, as our original plan was to concentrate our limited resources in the United States, albeit with organizations that have a global outlook. We have learned, however, that we need to work more broadly to signal not just the international community, but the domestic one as well, that we are not approaching cyber policy issues from a wholly U.S. perspective.

We will begin with targeted grantmaking in a handful of countries where our impact can be greatest. The effort thus includes examining different criteria to evaluate prospective countries, risk factors, and potential impact. We will weigh pros and cons and ensure that any grants proposed to the Board do not dilute our funds or stretch the Cyber Initiative's grants budget too thin. We will connect our U.S. grantees to any future international grantees to help build a more robust international cyber policy field and leverage our resources most effectively. This includes creating linkages between our U.S.-based university grantees and universities overseas.

STRATEGIC COMMUNICATIONS. Strategic communications is critical if we are to succeed. Because the Cyber Initiative is focused on field building, progress requires the organizations and individuals we support to communicate effectively: to make their voices heard in the public debates about cybersecurity and, in this way, to influence and improve the policymaking process. Over the course of the Initiative, we will seek to ensure that grantees have the capacity to communicate about their work and that they do so effectively, in alignment with our shared objectives. This means connecting grantees to key target audiences, amplifying their voices, and sharing their work through events, social media, digital content, and speaking engagements.

In support of our effort to mobilize more resources for the field, we will use our institutional communications channels to explain philanthropy's critical role in building a cyber policy field that serves the public interest.

GRANTEE ENGAGEMENT. We will hold our first grantee convening in early 2016, where we can ask grantees to react to our approach, weigh in on our proposed milestones, and help us think through how to evaluate our collective progress. We plan to involve grantees in designing the meeting's agenda to encourage their buy-in and maximize what we can learn from them. Following the Madison Initiative's success with a similar convening, we hope as well to use the gathering to encourage conversation and collaboration and build linkages among our grantees (which contributes to field/network building).

The importance of effective cybersecurity policymaking will only grow with time, as connected devices and emerging technologies continue to transform every aspect of our society. The Hewlett Foundation's Cyber Initiative is intended to help build a robust, multidisciplinary field that can inform that process in service to the public interest.

We will continue to work with our grantees, as well as experts from government, the private sector, civil society, and academia to support dialogue and the development of relationships of trust to help the field coalesce. Developing thoughtful solutions to complex cyber policymaking challenges will require the contributions of many individuals and organizations drawn from diverse disciplines and sectors. We are pleased to be able to support their efforts.

The resources we have made available as part of our initial five-year commitment are an important contribution to the development of this nascent field, but alone are not sufficient to address the scale and complexity of the challenge. We will continue encouraging our fellow funders to commit their resources to this important work.