THE WILLIAM AND FLORA HEWLETT FOUNDATION
Memorandum

Date: March 27, 2014

To: The Hewlett Foundation Board

From: Megan Garcia, Tom Steinbach, Larry Kramer

Subject: **A Proposed Cyber Initiative: The State of the Field and Hewlett's Potential Impact**

Last February, we began looking into the possibility of working in the cybersecurity field. This memo synthesizes our research, interviews with experts, and analysis of the subject. It provides a summary of our findings about the state of the field, what government and industry are doing to address cybersecurity challenges, and where and how philanthropy might make a difference. In short, policymakers and the public are looking for ways to engage in a discussion regarding how to make tradeoffs among numerous important and potentially conflicting values—including privacy, security, openness, innovation, profitability, and access. Yet no framework, place, process, or leadership exists to structure or facilitate that conversation, much less to find the right way to ascertain and implement the necessary tradeoffs.

There is, in other words, a significant need to build a cybersecurity field, and we request the Board's approval to spend $4 million per year for five years to begin doing so. This would entail finding or creating dependable, independent institutions capable of bringing together relevant actors from government and industry, and supporting and nurturing experts who possess a sophisticated understanding of the problem, are positioned to think about long-term policy needs, and will communicate and share information.

From a funding perspective, this new initiative would utilize money that has been supporting the Nuclear Security Initiative (NSI), which is winding down this year. The two are, however, unrelated. As you may recall from earlier discussions, NSI was created as a five-year initiative that would end in 2014. As it draws to a close, we will take stock of the lessons learned and share them with the Board and others. In the meantime, cybersecurity has emerged as a new and pressing problem in which we can make an important difference, though in ways distinct from our efforts in the nuclear security arena.

I. Why Cybersecurity is a Concern

The Internet plays a critical role in nearly every aspect of our lives—from government to commerce to personal communication. And by "our" in that last sentence, we refer to a global population: the number of Internet users worldwide, which nearly doubled between 2007 and 2013, is now estimated at 2.27 billion people. More telling, global Internet traffic is expected to *triple* over the next five years, with particularly rapid growth in Africa, Latin America, and the Middle East. In the meantime, smaller and more powerful chips and sensors are being embedded in more products, creating huge amounts of data and linking a vast and growing array of physical and digital systems. According to a report by the Council on Foreign Relations, the resulting "Internet of Things"—cars, ovens, office copiers, electrical grids, medical implants, and other Internet-connected machines that collect data and communicate—will encompass 31

billion devices by 2020.[1] It's an unprecedented development in human history, with incredible power and potential quality-of-life benefits. However, as General Michael Hayden, former director of the National Security Agency and the Central Intelligence Agency, noted in our interview, each of these devices is a potential point of entry for someone to steal intellectual property, shut down or damage critical infrastructure, or gather information for illicit or destructive ends.

It thus comes as no surprise that the growing importance of the Internet over the past two decades has included a corresponding rise in its use for criminal, intelligence, and military purposes. Attacks originating over the Internet are being launched against both private and public interests by a diverse range of actors motivated by an equally diverse set of reasons. The Government Accountability Office provides a succinct classification of the threats:[2]

> ***Threats to national security*** encompass attacks aimed at the systems and networks of the U.S. government, including the U.S. military, and attacks on private entities that support government activities or control critical infrastructure. Such attacks may be intended to cause harm for monetary gain or for political or military advantage. They can result, among other things, in the disclosure of classified information or in the disruption of operations supporting critical infrastructure, national defense, or emergency services.
>
> ***Threats to commerce and intellectual property*** include attacks aimed at obtaining confidential intellectual property for economic gain. In some cases, theft of intellectual property may also have national security repercussions, as when designs for weapon systems are compromised.
>
> ***Threats to individuals*** comprise attacks that lead to the unauthorized disclosure of personal information, such as taxpayer data, Social Security numbers, credit and debit card information, or medical records.

Each of these threats can be posed by any number of actors, including national governments, groups unofficially sponsored or enabled by national governments, bot-network operators,[3] hackers, criminal groups, or terrorists.

In discussing these threats, popular media often highlight the risk of all-out cyberwar. At present, only a few nations (Russia, China, Israel, France, the United States, and the United Kingdom) and a small number of the most sophisticated cybercriminals have the advanced capabilities to launch a cyberattack that could do the kind of damage needed to rise to the level of an act of war.[4] While this is a real concern, the broad problem of cybersecurity is probably better understood in terms of less visible, less dramatic events that nevertheless can,

---

[1] *Defending an Open, Global, Resilient and Secure Internet*, Council on Foreign Relations, Independent Task Force Report No. 70, June 2013.
[2] *Cybersecurity: National Strategy, Roles and Responsibilities Need to be Better Defined and More Effectively Implemented*, GAO-13-187, February 2013. For specific examples of each kind of threat and specific incidents see the GAO report.
[3] A bot-network (or botnet) is a set of remotely controlled systems that can breach computers to install malware that enables someone to control those computers remotely.
[4] James A. Lewis, *Conflict and Negotiation in Cyberspace*, Center for Strategic and International Studies, February 2013, page 4.

cumulatively, inflict serious harm to the economy and community or to individual safety and well-being.

As recent controversies make clear, cybersecurity intersects and overlaps with privacy concerns at many points—everything from government's desire to gather intelligence to industry's desire to protect trade secrets and customer information to individual expectations that private information will remain secure. The potential for conflict between security and privacy is pervasive, and any effort to work on cybersecurity must grapple with it. It is, however, too soon to have a firm position on what the balance should look like or even how to go about deciding. So while the issue of privacy will be an important part of any strategy, we do not believe it should be the principal lens through which the issues are understood, not yet at least. It is, rather, one among many considerations that must be sorted out.

II. The State of Play

The world of cybersecurity is changing rapidly—too rapidly in some respects. Technological innovation continues to be fast-moving, and the parts of government responsible for handling cyber issues (like the Department of Homeland Security) cannot keep pace with the changes. Even the more nimble private sector finds itself straining to keep up. At the same time, Congress and the larger public need help to understand the ramifications of the dramatic increase in cybersecurity threats.

A. Key Actors

The state of play in the cyber arena is unique. On the one hand, many threats have long been recognized, and there is, as a result, considerable activity aimed at thwarting them or mitigating the damage. On the other hand, this activity is sufficiently disparate and uncoordinated, and it leaves so many large and important gaps, that one is hard put to call it a "field."

1. Government activity. The U.S. government has become increasingly active when it comes to cybersecurity, though it has been reactive rather than proactive in addressing threats. The Department of Homeland Security (DHS) was assigned responsibility for securing critical U.S. infrastructure when it was created in 2002. Unfortunately, DHS is notoriously bureaucratic and is viewed as technically incompetent by industry and most of the experts we interviewed. Over time, the Departments of Commerce, Defense, Justice, and State have been called upon to work with DHS on efforts to develop international standards, formulate cyberdefense policy, facilitate overseas investigations and law enforcement, and represent U.S. interests in international forums. This has created confusion, and outreach to international agencies that handle cyber matters remains uncoordinated across the U.S. government.

Responding to the rise in cybercrime and cyberattacks on government systems, President Obama commissioned a "Cyberspace Policy Review" in 2009, declaring the cyber threat to be "[o]ne of the most serious economic and national security challenges we face as a nation" and stating that "America's economic prosperity in the 21st century will depend on cybersecurity." Later that same year, Secretary of Defense Robert Gates established the U.S. Cyber Command and gave it responsibility for defending military information networks against cyberattacks, and President Obama appointed a "Cybersecurity Coordinator" as Special Assistant to the President to address recommendations made in the Cyberspace Policy Review.

This past year witnessed a number of significant new developments. After fights in Congress over whether and how to constrain the sale of pirated material online, as well as high-profile attacks on the New York Times, the Wall Street Journal, and the Department of Defense's Joint Strike Fighter program, President Obama released an Executive Order on Cyber Security in February that created a voluntary information-sharing program between industry and government.[5] Also in February, the Department of Defense announced plans to increase the size of its Cyber Command by 2016 from nine hundred to several thousand. Partly as a result of extensive news coverage focusing on China's role in cybercrime and cyberattacks, President Obama made cybersecurity one of the top subjects for discussion when he met with President Xi at the Sunnylands Estate.

Finally, Edward Snowden's disclosure of classified NSA surveillance programs generated a wave of government and industry activity. President Obama introduced small measures of transparency into NSA protocols and is rumored to be considering more meaningful changes in the Agency's operations. The Snowden leaks also generated a number of lawsuits challenging the constitutionality of the NSA's surveillance programs. Finally, Snowden's revelations stoked enormous public interest in the scope of programs designed to prevent terrorist attacks, such as the NSA's mass collection of cell phone data. This spike in public interest offers a much-needed opportunity to begin a richer, more dynamic national conversation about how cyberspace should be governed.

Government funding has been commensurate with these activities. For example, the NSA provides money to select universities (designated "Cyber Centers of Excellence") to train cyber experts that the agency can then hire. The Department of Defense is reportedly spending $23 billion on cybersecurity activities from 2014-2019. These funds will be divided between internal activities in Cyber Command and outside contractors hired to develop new offensive and defensive capabilities. Finally, the Department of Homeland Security has a 2014 budget of $500 million for cyber-related research and development alongside almost $8 billion for capital improvements and protecting critical infrastructure.

Obviously, these are important priorities. But spending on this scale, for a problem of this importance, should be guided by policy frameworks that were developed with a deep understanding of the problem and that take long-term consequences as well as immediate needs into account. No such frameworks exist at present. And, unfortunately, many of the government officials we interviewed told us that few if any resources are being used to develop them.

2. Industry activity. The private-sector cybersecurity landscape is complex, with a great deal of variability in the maturity and sophistication of different organizations' cybersecurity programs. Like government efforts, however, private-sector efforts to grapple with cyber problems are largely reactive, driven by immediate and short-term interests and needs.

To learn more, we commissioned the consulting group iSEC Partners to conduct a survey of industry cybersecurity practices. They conducted interviews with banks, large and small technology companies, telecommunications companies, healthcare organizations, and organizations in the energy sector.

iSEC Partners identified a number of ways in which cybersecurity in the private sector needs to be improved. Most prominent among these was a need for greater information sharing, both

[5] For the full text of the Executive Order, see http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity.

among private enterprises and with government. Sharing information about cyber incidents is critical to preventing attacks and developing enduring defenses, yet it remains very rare. Information sharing among companies needs to be more transparent and reciprocal, and the information shared needs to be of a higher quality (providing more detail on the techniques used, for example, as opposed to simply sharing an attacker's easily changed IP address). The same thing is true when it comes to information sharing with the government. Private-sector interviewees uniformly bemoaned how interactions with the U.S. government are one-sided, based on government demands and unhelpful to them.[6]

To improve information sharing, trustworthy—and trusted—information-sharing systems need to be built. Such systems cannot be built by government or even by industry trade organizations, both of which suffer from suspicions about bias. This is an area in which the non-profit sector might be able to play a useful role due to its perceived neutrality.

iSEC Partners identified four other areas of need that, while less pressing, potentially offer additional avenues for grantmaking. These include educating both non-technical employees and consumers about cybersecurity; enhancing research on defense from cyberattacks; protecting critical infrastructure; and helping to develop open source software to enable smaller companies to protect themselves from cyber threats.[7]

3. Advocacy organizations and academics. While cybersecurity has become a catchphrase among national security experts over the past few years, very few independent advocacy organizations are working thoughtfully on the issue. Such activity as currently exists tends to focus on protecting consumer privacy. For example, the ACLU worked hard to defeat legislation that would have allowed the NSA to ask private companies for information about customers' Internet use without removing personally identifiable information, and the Electronic Frontier Foundation (staffed by a mix of lawyers, technology experts, and activists) has brought numerous lawsuits against the federal government to limit the NSA's activities in the interest of privacy.

Interest in cyber issues is beginning to grow among some think tanks, but none has yet taken on the task of developing a comprehensive conceptual framework for cybersecurity. The small amount of cybersecurity funding that goes to NGOs and think tanks comes mainly from private companies, moreover, which skews the work toward thinking about how government actions affect industry rather than about the landscape as a whole and leaves the results vulnerable to attack as biased. As with government and industry, most of the research is reactive, and no one is thinking broadly or systematically about a larger framework or about what cybersecurity should look like in the future.

---

[6] Interestingly, many of the same interviewees reported having nondisclosure-protected meetings with foreign governments in which there was two-way information sharing of a type they said simply does not happen with the U.S. government. The companies believe foreign governments make a greater effort to share information to attract or retain business. That in turn allows the companies to use their expertise to help government officials better understand cybersecurity.

[7] Open source ventures also help facilitate collaboration across industry, academia, and government. One such project, the Open Web Application Security Project (OWASP), was singled out for praise by multiple interviewees for its impact on general security education and for the resources it provides. The Open Web Application Security Project (OWASP) website is: https://www.owasp.org/index.php/Main_Page.

B. Key Problems

We identified three overarching problems in the current cybersecurity field: (1) the field is fragmented, making it difficult for relevant actors to work together; (2) the field lacks thought leadership that can keep pace with fast-changing policy decisions and other developments; and (3) the technical nature of the issues makes the threats difficult for the general public and policymakers to understand.

1. The field is fragmented. As mentioned above, the various actors thinking about and working on cybersecurity issues—the intelligence/national security community, policymakers, NGO activists, academics, and people in industry—are not working together and have surprisingly little interaction. They approach the problem differently, have different beliefs about the role government should play in tackling problems, and even use different language to describe overlapping concepts. "Cybersecurity" is the term most often employed by government officials to describe the security of computer systems and networks. Technical experts and many in industry favor "computer security," while other experts and most private-sector actors use terms like "information security" or "infosec."

These differences in language may seem trivial, but they have consequences. In some instances, the different terminology reflects disagreement about the priorities various actors give to different types of threats (whether from industry actors in other countries, from spies, from hackers, and so on). We were surprised in our interviews to observe the extent to which terminology has become a barrier that limits or confuses cross-sector discussions among people in industry, government, the intelligence community, and academia. In essence, the terminological confusion reflects the extent to which the field—by whatever name—is not yet sufficiently developed to have a set of definitions that a majority of experts and practitioners accept.

2. There is a lack of thought leadership. Almost everyone with whom we spoke, both inside and outside government, commented on the cybersecurity field's lack of thought leadership. Most could name no more than one or two people—usually the same people—to whom they might turn if they needed to brainstorm or bounce ideas around. In addition, many of those working on cybersecurity issues have technical or purely academic backgrounds and are poorly positioned to understand the full suite of complex issues involved in cybersecurity. There also is a marked shortage of people with the right combination of political acumen and technical knowledge needed to help guide the difficult, sophisticated decisions that need to be made.

3. The technical nature of the problem has inhibited action. While there has been a sharp increase in media attention to cyber threats in the past two years, producing greater public awareness about cybersecurity, the technical nature of the problems has kept the public and most policymakers from fully understanding and embracing potential solutions.

III. A Role for Philanthropy

A. The Current Funding Environment

As we have seen, while government and industry both spend a great deal on cybersecurity issues, their work fails to address important questions and problems. Government is focused chiefly on building offensive and defensive weapons and systems, while individual companies erect ever-higher walls to minimize theft and government interference. Few resources are

devoted to thinking about cybersecurity from a broad public policy perspective. Neither government nor industry has invested in developing independent thought centers or leadership or has funded efforts that do not advance their immediate, narrowly conceived interests.[8]

B. A Role for the Hewlett Foundation

1. Focus and theory of change. Our theory of change for this initiative is that by funding activities and information-sharing systems that (a) support and encourage independent research from a broad policy perspective, and (b) bring together government, private-sector, and nongovernment cybersecurity actors, we can increase trust and coordination among the key players and improve the quality of debate. This increased trust and improved discussion will, in turn, help cultivate a cybersecurity field capable of tackling substantive cyber problems that currently sit outside the ambit of any of these actors on their own.

Although the Internet and problems related to its use are inherently global, our funding would at the outset focus on institutions based in the United States. There are more than enough of these to absorb our funding, and focusing this way is more likely to generate the collaboration and information sharing we view as essential.

2. Goals. While we believe the Hewlett Foundation can play an important role in building a cybersecurity field, we do not believe we can do this alone, certainly not without spending considerably more than $4 million per year. Our objective is to act as a catalyst by leading the way, showing what can be done, and, in this way, spurring other foundations and funders to enter the sector while encouraging government and industry to widen their focus. We will do so by pursuing the following four subgoals:

> ***(a) Begin to develop a network of cybersecurity experts.*** We would make grants to foster connections among experts from industry, government, think tanks, academia, and elsewhere, encouraging collaborative work as well as better information sharing and communication. Within five years, we would also hope to see industry and government begin to fund organizations we have seeded or supported for these purposes.
>
> ***(b) Help individuals and institutions develop comprehensive analyses of cybersecurity problems and solutions.*** It is still too early, and we still know too little, to promote a particular normative or conceptual solution for cybersecurity. Rather, our initial grants would aim to encourage sophisticated thought leaders—coming from different sectors and bringing different professional, political, and intellectual perspectives—to begin developing frameworks that can guide the analysis of such unanswered questions as, Who should govern the Internet? What values should underpin national and/or international cybersecurity policy? What information should industry and government have access to? How should government do long-term cybersecurity planning? A marketplace of ideas and robust intellectual debate among experts from different sectors working together would constitute an important first step toward developing sensible norms and rules for cybersecurity.

[8] As one interviewee put it, the field is presently much like nuclear security before Thomas Schelling and others developed a general conceptual framework for thinking about problems of nuclear deterrence. Indeed, a number of interviewees expressed concern that many in the defense establishment are unthinkingly extending the nuclear framework to this new threat despite manifest differences that make it inappropriate and possibly dangerous.

(c) Attract new funders and additional funds. A number of funders with whom we spoke acknowledged the importance of cybersecurity and said they wanted to engage, but admitted to being daunted by the size, scope, and complexity of the field. We believe we can allay their concerns by demonstrating through projects we fund that it is possible to make a difference, using our early grants as examples of meaningful entry points. At the same time, we have begun (and will continue) talking directly to other foundations about collaborating.

(d) Fill critical research gaps. A shortage of credible information and independent research about cybersecurity problems forces policymakers and business leaders to make important decisions based on best guesses rather than data and informed analysis. We would seek to fill this gap by supporting research; identifying the circumstances under which business and government agencies will use it; looking for ways to connect researchers to key decision makers; and helping launch or grow institutions with the necessary technical, policy, and business expertise to disseminate ideas and foster public debate.

CYBER SECURITY STRATEGY: FIVE-YEAR GOALS

FIVE-YEAR GOAL	Examples of what we will fund	Sample Grantees	Problems this would address
BEGINNINGS OF A NETWORK EXIST	Meetings, incubators, applied research on elements of successful networks, crowdsourcing	IDEO, Summit Series, TED	• Fragmentation of the field and little interaction between key players • Private entities not adequately sharing information with each other • Lack of thought leadership, shared language, and understanding of the full suite of complex issues
EARLY SIGNS OF A FRAMEWORK TO ADDRESS CYBERSECURITY	Analysis of current efforts, Cross-sector efforts to create frameworks	CISAC, Berkman Center, CNAS, New America Foundation, CFR	• Lack of thought leadership, shared language, and understanding of the full suite of complex issues • Technical nature of the problem • Capacity must be sustainable
MORE FUNDERS & MORE FUNDS	Philanthropic funder outreach (Hewlett Foundation staff to do directly)	NA	• Lack of projects aimed at thinking about the big picture of cybersecurity
CRITICAL INFORMATION GAPS FILLED	Research	Academics, think tanks	• Lack of thought leadership, shared language, and understanding of the full suite of complex issues • Technical nature of the problem • Proprietary nature of some research • Precarious nature of media coverage and public awareness, which ebb and flow with crises

3. Evaluation. Given the newness of the field, we will need to experiment with different kinds of grantmaking while monitoring what happens closely so we can learn and adapt as the initiative proceeds. To that end, we plan to incorporate an evaluation process from the outset and to monitor our work in real time. In addition, we propose working with an outside evaluator to assess our efforts at building a cybersecurity field after two years and again after five years.

Initial evaluation questions include the following:

Network: 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?

Frameworks: Have new conceptual frameworks been developed for thinking about and addressing cybersecurity problems? Are leaders emerging who can galvanize thinking about cybersecurity? If so, where and why? If not, why not?

Funds: Have more philanthropic funders and funds been attracted into the cyber field since we began funding? What is the best way to stimulate funders to enter the field or increase their funding?

Information gaps: Have the organizations we funded produced high-quality research? Is the research considered credible? Are policymakers and industry using it for decision making? If so, how? If not, why not?

Given how much may change over the course of the proposed five-year initiative, it may be the case that we ascertain that we are not having impact, that we are having more impact than we thought we could have, or that we must dramatically change course. Because of this uncertainty, we propose to make our plans for exit a part of the ongoing discussion we have with the Board about what we are learning and how much impact we are having.

4. Key risks. In addition to the usual audience of academics and policy experts, the population of people who can drive new thinking in cybersecurity includes technologists, start-up owners, information security practitioners, and young hackers—groups with whom we have little experience, yet whose buy-in will be critical to success. Other risks include the possibility that industry and government do not want independent research about cybersecurity, that cybersecurity experts in different sectors have no interest in interacting with each other, that the organizations we fund are not capable of bridging the gap between industry and government, and that other funders will prove uninterested or unwilling to enter the cybersecurity field.

Based on our research to date, we believe these risks can be overcome, though we are eager to test our assumptions and ready to adjust if they prove wrong. On balance, we believe the risks are justified given the enormous value that will be generated if we succeed.

An overarching risk comes from the dynamic nature of the problem, which makes this a difficult field in which to work. Even apart from the rapid shifts produced by disparate actors tackling short-term problems without consulting or sharing information—something we hope to begin to redress—we must keep up with the dizzying pace of change in technology itself. Changes in technology are constantly reshaping the nature of the threats and potential for solutions, as well as giving rise to new problems. Our work must keep abreast of such changes, and we are building a monitoring and evaluation plan into the strategy that will provide us with nimbleness and flexibility to respond to these changes.

IV. Conclusion

The cybersecurity problem is incredibly mutable and unsettled. Government cannot keep up with changes taking place in the private sector, while industry plunges ahead wearing blinders of immediate interest and Congress and the public struggle to understand the ramifications of cyber activity that is increasing at a daunting pace. And all this is taking place against the backdrop of a fractured field of experts and practitioners who do not communicate well or often.

The Hewlett Foundation has an opportunity to engage these disparate players, learn from them, and experiment with new approaches to field building. Cybersecurity represents an exciting opportunity to advance a field that needs attention but is largely new to private philanthropy. If successful, our efforts will yield important security benefits to individuals, communities, businesses, and the international community. It's an uncertain bet, but one surely worth exploring.