Special Cyber Initiative Grants Memo

THE WILLIAM AND FLORA HEWLETT FOUNDATION
Memorandum

Date: November 4, 2014

To: Board of Directors

From: Larry Kramer

Subject: Cyber Initiative Grants to UC Berkeley, MIT, and Stanford

This memo explains the basis for three special grants we are recommending in the November docket. The grants, proposed in connection with the Cyber Initiative, are for $15 million each to the University of California, Berkeley; the Massachusetts Institute of Technology; and Stanford University. The discussion below explains the basis for our recommendations, describes the proposals, and considers associated benefits and risks. The full proposals, which are rather lengthy, are in an appendix in the Board Book.

I. Introduction

Last March, the Board approved a new "Cyber Initiative" with a budget of $20 million over five years. The Initiative aims to build a field of policy analysis for problems relating to security and technological trustworthiness on the Internet. While government and industry are both already spending vast sums of money to deal with such problems, their focus is overwhelmingly on present needs and problems and mainly involves developing technologies to combat hackers, thieves, and enemies. Hardly anyone is thinking about the lasting consequences of today's solutions, much less about developing overarching policy frameworks for long-term global governance and security.

The importance of having such frameworks cannot be overstated. Our lives increasingly depend on the Internet, and choices we are making today about Internet governance and security have profound implications for the future. To make those choices well, it is imperative that they be made with some sense of what lies ahead and, still more important, of where we want to go. Yet little or no thought is being given to such questions, partly because of avoidable obstacles. At present, few institutions treat questions of cybersecurity and Internet policy as a central or even important focus of their work. Individuals with proper training to address these questions are in short supply, and those who exist seldom speak to each other or share information. Nor has anyone given them reason to do so: funding for this sort of work is practically nonexistent.

The Cyber Initiative seeks to overcome these obstacles, and, in so doing, to build a "marketplace of ideas" about cyber policy—generating the kind of robust arguments and analytic frameworks needed to begin articulating sensible long-term public policy. We plan to do this by (1) supporting and/or building dependable, independent institutions capable of training, nurturing, and supporting experts with a sophisticated understanding of the problems; (2) convening experts from government, industry, academia, think tanks, and other arenas to share

information and develop the trust needed to work collaboratively; and (3) attracting additional funders to help grow and develop the new field.

The announcement of the Cyber Initiative prompted a great deal of commentary about the need for, and importance of, our plan—much of it likewise emphasizing the absence of serious public policy analysis. These reactions came not just from potential grantees (whose statements may perhaps be taken with a grain of salt), but also from people working in government, industry, the media, and philanthropy. Our specific focus—creating opportunities for people coming from different sectors and disciplines to exchange information and work together, and developing multiple long-term policy options—was singled out for particular approbation. Given the modest size of the initiative, the attention it garnered came as a pleasant surprise, but it also says something about timing: public policy for cyber is a field ripe to be built.

Even so, building the field will not be easy—and not just because of the modest scale of our initiative, which is only $4 million per year for five years. As we explained to the Board in March, our plan has never been to build the field ourselves. Rather, we intend through our grantmaking to demonstrate what is possible, while working to attract additional funders and funding into the field. The reactions to our announcement were heartening precisely because they confirmed our sense that there is widespread interest and curiosity. The bigger problem turns out to be that the field is so underdeveloped that neither we nor other potential funders have adequate places even to begin.

An unanticipated partial solution to this last problem emerged during the summer, with the discovery that the Foundation needs to pay out more this year than originally budgeted if we want to keep the excise tax on our earnings at one percent. The Board agreed in July that we should do so. In September, I updated the Board, explaining that the Foundation needs to spend as much as $50 million before December 31 for this purpose; at the same meeting, the Board agreed to allocate $5 million of this amount for humanitarian aid in connection with the Ebola outbreak in Africa. Those funds are in the process of being disbursed.

At the time of the July meeting, the Board agreed to consider using the remaining funds in connection with the Cyber Initiative. More specifically, the Board gave permission to ask three Universities—Berkeley, MIT, and Stanford—to submit proposals for grants to establish multidisciplinary, public policy programs focused on cyber issues broadly understood.

It is worth briefly recounting the reasons behind this decision. As we discussed in July, establishing a number of strong academic centers will powerfully kickstart our Cyber effort—making a potentially transformative difference in launching a new field of public policy analysis. These grants will create critical centers of excellence that give other funders places to start building and enable us to use our limited resources more effectively. And if prior experience is any guide, we can expect other universities, think tanks, and funders to follow suit in launching their own cyber efforts.

A second, more easily answered question is, why Berkeley, MIT, and Stanford? To begin, it makes sense for us to start with major research universities. Eventually, we will need to

support think tanks and other potential homes for policy development, including institutions that can attract participation from quirky and unorthodox technology types. But universities are likely to remain the foremost centers for developing long-term policy analysis, especially as our goal is to support analysts who are independent of both government and industry. Universities will also remain the key destination for training new people. Finally, and especially relevant for present purposes, major research universities are among the relatively small set of institutions capable of absorbing and making good use of $15 million grants in short order.

There were, of course, other universities to consider in addition to Berkeley, MIT, and Stanford. Based on our research, however, the three schools we selected seemed like the most promising place to start. All three have concentrations of world class faculty and graduate students working in a variety of relevant programs and centers scattered across their campuses—programs and centers that could and should be aligned to work collaboratively on cyber issues. What they have lacked are the resources and the impetus to do so, which the proposed grants will supply.

II. The Proposals

A. Process

A few days after our meeting in July, I called the presidents of Stanford and MIT and the chancellor of Berkeley to invite submissions. Our timing, it turned out, was fortuitously perfect. All three universities had begun internal conversations about cyber policy that were bogged down and disorganized; our initiative and the prospect of a substantial grant gave them a timeline and focal point that kicked things into high gear. Multidisciplinary teams were immediately formed to develop proposals at all three schools, with strong support from university leadership. We put the team leads in touch with each other, so they could share ideas and information, but we told them they should feel free to act independently in developing proposals, as we want each university to determine its strengths and interests for itself.

The ensuing process was quite intense as these things go, propelled by the short timeline we gave the universities to develop and submit final proposals. Constrained by the need to make these grants before yearend, the time pressure turned out to be productive, as it forced everyone to focus and be constructive at meetings and in conversations. We stayed in close touch with all three teams, speaking almost weekly to ensure they remained on target and on track. We were careful not to exercise too much control over the substance of the proposals, imposing only the following general conditions: (1) that the proposals establish a university-wide center or program focused on public policy in the cyber arena, (2) that there be an emphasis on medium to long-term policy concerns from a societal and global perspective, and (3) that the center or program be multidisciplinary and provide incentives for people from across the university to work together, embracing some mix of science, engineering, the social sciences, and the humanities. These were not difficult conditions, as they matched the preferred approach of all three universities anyway.

Within that broad framework, we left each university free to develop the proposal that best suited its perceived strong points. Once we knew the amount of available funds, we told

them they could submit proposals for up to $15 million. Other than requiring that funds be expendable and not used for endowment, we gave each university leeway to determine the rate and pace of spending. In addition, we asked all three universities to include plans for communications and for continued fundraising from alumni and other sources.

The teams at all three universities held numerous meetings between late July and mid-September to develop their approaches. It is fair to say that the process itself had the effect of generating added excitement and drawing in additional faculty. The universities shared their proposals with each other and exchanged ideas along the way. An unanticipated benefit of this sharing is that the three institutions have already made plans to collaborate with each other if their proposals are approved. I remained in contact with Presidents Hennessy and Reif and Chancellor Dirks to ensure the continued enthusiasm and support of university leadership—which we have.

We reviewed the submitted proposals carefully. Megan Garcia, Tom Steinbach, Angela Whitney, and I each read and commented separately. I also sought independent reviews from three trusted outside readers. Reactions were uniformly positive, accompanied by a variety of suggestions to improve or clarify the proposals. The universities willingly incorporated these suggestions. It was an effective and productive process, despite its unusual speed, as evidenced by the high quality of the resulting proposals.

B. Content

The central activities these grants will enable are similar at all three universities. Basically, we want and need them to do in the cyber arena the kinds of things great research universities do best: support innovative research, educate and train scholars and practitioners, develop and teach classes, and convene diverse stakeholders to share ideas and information. In so doing, each university will support and advance all the goals of the Cyber Initiative. This is philanthropy of a traditional sort: a kind of grantmaking that has always been in the Hewlett toolkit. Rather than ask grantees to specify particular outputs, we are building institutions—providing generous support to organizations we trust to launch ventures that will chart an evolving course whose general direction is known but whose final destination will be determined by the grantees as the journey proceeds.

We did, as noted above, ask our would-be grantees to satisfy a few basic conditions. In terms of substance, the grants are meant to stimulate policy analysis of problems arising from activities on or related to the Internet. This does not preclude using funds for other cyber-related purposes, such as developing technology, but only in support of understanding or addressing problems of public policy. We further asked the universities to look beyond the worries of the moment and to think in terms of a longer time horizon, which is where the largest gap exists in current thinking. Once again, this does not prohibit working on immediate or short-term problems as part of the larger project and with the long view in mind.

Such minimal conditions leave room to address an enormous range and number of issues, encompassing everything from privacy, security, and governance to business practices, consumer welfare, war, intellectual property, and more. We did not oblige the universities to

limit or commit themselves to any particular subset, because we hope and expect these programs to last for years, and we want them to grow and change as circumstances dictate. At the same time, recognizing that some kind of initial focus is needed to lend the projects coherence and bring people together, we asked the universities to identify a substantive starting point and describe the kind of research and other projects they expect to support at the outset. Each university responded by coming up with something a little different, as discussed below.[1]

We imposed two structural conditions as well. First, we asked that the program or center have its own physical space. This may seem ironic as applied to a cyber-center, but entities like this are much more likely to thrive in the university environment if they have a distinct physical home. Second, we required the proposals to be multidisciplinary and to draw on intellectual resources from across the university. We were clear, moreover, that this meant more than supporting research and teaching in different disciplines. We mean to encourage and facilitate collaboration among faculty and students in different disciplines, not to funnel support to multiple silos. Fortunately, this interest is strongly shared at all three universities, though we still dedicated considerable time to discussing with each exactly how they planned to achieve this goal.

When all is said and done, leadership is by far the most important ingredient for success in a venture of this sort. Even if it were possible to specify everything in the initial proposal, it would be a mistake to do so. We are, after all, inaugurating programs that are meant to be organic and that we want to develop and evolve with the new field of cyber policy they will be instrumental in creating. Whether the programs flourish thus depends first and foremost on the quality of the people in charge, and we carefully investigated the leadership teams to make sure they are up to the task. This turned out to be hardest at Stanford after the person we initially hoped would oversee its program was appointed to the California Supreme Court (I mean, of course, Tino Cuéllar). Fortunately, Stanford is a strong university with a deep bench, and they quickly came back with an unconventional and imaginative alternative (George Triantis), backed by a superb Steering Committee. We are, as a result, confident in the leadership at all three universities.

As noted above, we pushed the universities to develop distinctive proposals, drawing on their particular strengths and reflecting the interests of their faculty, staff, and students. The teams shared information and communicated with each other, but in the end—as we hoped—each university developed its own, unique plan. I describe these briefly below:

1. The University of California, Berkeley. Like the other proposals, Berkeley's proposed Center for Internet Security and Policy (CISP) will use the funds we provide to support a full array of activities, including research, curriculum development, seminars, conferences, outreach beyond the university, and more. They propose to organize these activities around what they see as the biggest obstacle to thinking clearly about the Internet's future, namely, uncertainty:

[1] We regard these differences as an important benefit of the grants—each likely to attract interest and attention from different parts of the cyber world, leading cumulatively to much broader reach across the whole space.

> Today, it is straightforward to logically construct a world in which literally everything, living and non-living is connected to the network in some fashion; it's just as straightforward to logically construct a world in which governments have brought the network under full sovereign control and tightly manage inputs, outputs, connections, and applications . . . . Those may be the most obvious scenarios at the extreme ends of a particular continuum; they're merely illustrative because that continuum, which seems most important and uncertain to many observers right now, may turn out to be less impactful than others, for example variance over how machine learning, robotics, and artificial intelligence evolve; or how militaries work out their conflicting interests. In fact, a wide variety of alternative possibilities are possible and even likely.

They propose to deal with this problem by organizing CISP around assessing "the range of possible future paths of 'cyber' and 'security,' and [bringing] these together into a *manageable set of scenarios"* (italics in original).

As a practical matter, this entails using the first year to develop scenarios through biweekly working sessions involving faculty from multiple disciplines, further informed by regular "summits" with representatives from government, industry, and civil society. This first phase is then followed by a second, involving seed grants for a diverse set of exploratory research projects "to identify and explore potential solutions to the challenges envisioned in the scenarios." Findings will be presented at a weekly campus-wide research seminar. Faculty would also be eligible to receive financial support to develop and teach new cyber-policy related courses.

"By the third year," the Berkeley team says, "we should have sufficient understanding of the field to begin funding larger scale research projects." CISP would thus identify up to five core areas for deeper research, making one or two awards annually for two-to-three year projects in each area. This phase would also see the launch of an annual CISP Research Symposium and white paper series, accompanied by a variety of communication tools to showcase the findings and make the research available to outsiders in Silicon Valley, Washington, D.C., and elsewhere. These various programs for teaching, research, conferences, and symposia would then continue on an ongoing basis.

CISP will be physically located at the Berkeley School of Information, led by an Executive Director reporting to a team of five faculty with joint appointments encompassing the Schools of Engineering, Information, Law, Public Policy, and the Department of Political Science. The proposal also includes plans for outreach to a wide range of external stakeholders, including outside experts, industry actors, government officials, potential donors, and so on.

2. The Massachusetts Institute of Technology. MIT proposes to develop a field of cyber policy from a different starting point: "Imagine trying to shape environmental policy," they muse, "if we had no way of measuring carbon levels and no science to assess the cost or effectiveness of carbon mitigation." This, they argue, is the state of cyber policy today: "growing urgency but no metrics and little science. The field is full of activity but highly immature."

Through an extensive program of collaborative research, teaching, conferences, and more, they propose to launch the MIT Cybersecurity Policy Initiative (CPI). With Hewlett's grant dollars, CPI aims in the next five years "to have created basic quantitative metrics and qualitative models that will allow policymakers to engage in a richer dialogue on these issues. And we will have trained a first generation of students and scholars who will lead research and action in this area to maturity."

CPI will be constructed around three core disciplines in which MIT is particularly strong: engineering, social science, and management. It will bring together scholars and practitioners from these disciplines to help inform policy in and through a four-phase process:

1. *engage* with industry, governments and citizens groups;
2. *explore cybersecurity* problems to understand the competing policy objectives, barriers to progress, and approaches that can lead to better security, including designing policies and technologies *in vivo* in an iterative manner;
3. *analyze* and generalize from these specific studies, drawing on a variety of social science and engineering disciplines, and anticipate impact on technology and policy development; and,
4. *educate* students to tackle these challenges in both academic, industrial and public sector settings.

MIT's proposal outlines an illustrative series of potential starting projects designed to address "key challenges." While the projects are all interdisciplinary, they fall into three clusters—each emphasizing contributions from one of the three key disciplines around which CPI is organized. Resources for these (or other) projects will be allocated by an interdisciplinary Faculty Steering Group whose task it will be to develop a comprehensive research agenda. In addition to regular faculty, MIT plans to support at least two visiting fellows as well as postdoctoral fellows and graduate students. Its plans also include an Advisory Board of representatives from government, industry, and civil society.

In addition to identifying the key research questions, the Faculty Steering Group will be responsible for using CPI's resources to "establish patterns of cross-disciplinary collaboration." They expect to spend the first year mapping out a research agenda with faculty and in consultation with government and private sector experts and colleagues at Berkeley and Stanford. The research agenda will be updated continuously through a process that includes an annual retreat. In addition:

> Throughout the life of the Initiative, we will host and co-host conferences and workshops both targeted at scholarly work, and to enable dialogue between industry, government, civil society, and academia. Based on preliminary discussions with potential Hewlett cybersecurity policy centers at Stanford and Berkeley, we plan to work together to organize an annual academic conference. In at least its first few years, we would expect to run this conference more in workshop style, helping researchers to prepare papers for publication in a variety of journals and conference proceedings in their own disciplines. We take as a very

> successful model, the Privacy Law Scholars Conference (PLSC). Like PLSC, our Cybersecurity Policy Scholars Conference would gather scholars from a variety of disciplines, all of whom share common subject matter. Such a conference could also host a paper and discussion track specifically targeting government, industry, and civil society participation.

Finally, MIT plans to expand the University's cyber related curricular offerings and student research opportunities with an eye to creating a new concentration in cybersecurity policy. MIT also details plans for communications and subsequent fundraising.

3. Stanford University. Stanford proposes to use our grant to create what they call the Cyber-X Initiative—"X" being a variable that can stand for any other discipline or relevant collaborator. The proposal resembles Berkeley's and MIT's in its emphasis on research, education, and engagement with stakeholders beyond campus. As the submission explains:

> The initiative will draw on Stanford's extensive experience with multidisciplinary, university-wide initiatives. At Stanford, a university-level initiative (vs. a school- or institute-based initiative) is a campus-wide "hub" and mechanism that (1) brings together scholars from multiple disciplines to discuss and define relevant questions that can be solved only through collaborative effort and understanding, (2) supports and facilitates the original research needed to address such questions, and (3) serves as a convener and implementer for wider engagement, within and outside the university, to further the conduct of that research as well as the dissemination and ultimate application of the research results. The goal is to promote university-wide faculty engagement and educational efforts; leverage current centers of excellence such as the Department of Computer Science, CISAC at the Freeman Spogli Institute, and the Center for Internet and Society at Stanford Law School; and break down disciplinary silos while allowing decentralized innovation across relevant campus units.

Where Berkeley has organized its work around scenario planning and MIT around developing metrics and models for analysis, at Stanford the work will focus around two substantive themes: trustworthiness and governance. These are "explicitly meant to cut across key issues and concerns that are often recognized as important yet in some cases treated separately, such as privacy, governance, international security, cybercrime, and the social and economic consequences of societies' increased reliance on networked, vulnerable computers." Stanford's plans are on a slightly faster time frame than the others, and they plan to use these substantive themes to guide the first three to four years of Cyber-X.

Trustworthiness encompasses more than security and refers to the fact that "people want and need information technologies to do what they are supposed to do and only when they are supposed to do it, and they want these things to be true in the face of deliberately hostile or antisocial actions." Figuring out how to achieve systems that are trustworthy is a problem that reaches beyond technology, implicating economics, law, politics, policy, psychology, organizational theory, and sociology, as well as computer science. It implicates the users of technology as much as its creators and abusers and frames a set of questions that encompass

things like building a safer infrastructure and developing domestic and international norms to manage the risks of conflict.

Governance is a similarly critical problem, though only Stanford has proposed to put it front and center. To make the Internet work, we must sort out and allocate responsibility among competing actors: governments, militaries, businesses, individuals, and civil society groups. All these actors have a stake in the architecture, deployment, policy, and operation of cyberspace, but there is too little research about who should do what. There is, moreover, still less work about how we might get actors to agree to and comply with such decisions—questions that include formal legal and institutional codes but extend well beyond these to include social norms, politics, and the dynamics of social interactions.

Stanford's proposal overlays these two substantive themes with an intellectual framework built around the concept of "emergence": the idea that the most important societal implications of a technology are seldom those contemplated when it is introduced but tend instead to emerge over the course of its use. Initial, usually intended, effects are most often economic in nature (increased productivity, reduced cost, etc.), whereas the later, often unintended, but more important effects tend to be social and cultural (fewer face-to-face interactions, more dispersed social networks, etc.). Approaching cyber policy with this framework in mind is, Stanford says, "important to designing better technologies and policies, and anticipating potential impacts on individuals, institutions, and our society more broadly."

Cyber-X will be housed at the Freeman-Spogli Center for International Studies. It will be led by a faculty chair, who will in turn be assisted by two multidisciplinary committees: a Steering Committee to provide strategic guidance, and a Grants and Fellowship Committee to oversee the awarding of research support. Both committees will include graduate students as well as faculty, an atypical feature we really like, and there will also be an outside Advisory Board to take advantage of Stanford's far-reaching network of alumni in technology, business, government, and international affairs. Stanford's proposal lays out an ambitious plan for faculty seminars and conferences, the creation of infrastructure to support broad dissemination of research, fellowships, the possible creation of a new degree program, and a variety of curricular innovations. They have equally ambitious plans for external outreach, including "public lectures and seminars, newsletters, reports, professional training, videos, and social media discussion forums, all of which can contribute to education and increased understanding across stakeholder groups in this field."

4. Measuring Success

Given the goals of these grants, as described above, we will track a number of discrete indicators to determine whether they have "worked." These include:

(a) Cross-disciplinary research synergy. A successful initiative will yield tangible examples of cross-disciplinary research projects executed by teams of faculty, staff and students from both engineering and social sciences. By 2020, this research should be appearing in leading journals and other publication venues—including at least some new vehicles created as a result of the initiative. A negative indicator here would be that authorship of publications

remains balkanized in single disciplines.

(b) Impact on public policy dialogue. One of our key aims is to make a positive contribution to the public policy debate in the United States and globally. A measure of success will thus be that conceptual frameworks, formal models, data, and policy analysis developed at the three universities are being used in and contributing to debate in policy venues around the world. We are not demanding specific legislative outcomes, but new research produced by CISP, CPI, and Cyber-X should play a role defining the terms and themes shaping policy debates. If the research never goes farther than academic journals and conferences, we will have failed.

(c) Building trust across sectors. We expect all three universities to play a role convening actors from government, industry, NGOs, and the technology sector, as well as helping to facilitate work and information sharing among and between them. Follow-up is as important as initial meetings for this purpose. We thus will have failed if these actors do not continue sharing information or develop ongoing relationships afterwards. We also will be looking to see some of these relationships take on institutionalized forms within and across different sectors.

(d) Developing educational pathways. The long run creation of a new field of study can only be considered complete if there are clear pathways for students at all levels of study and in all relevant disciplines. We should learn a lot in the first few years about how to prepare students for work in this field, whether they choose career paths in academia, government, industry, or civil society. By 2020, the universities should have many of the essentials for such programs in place, including a growing set of classes, rich faculty-led research opportunities, and significant faculty interest in the field.

C. Benefits and Risks

While many benefits can be expected to flow from these grants, they can be summarized relatively quickly. People throughout government, business, academia, and think tanks have long recognized how many critical public policy issues need to be dealt with to make the Internet safe and functional: this is emphatically not a new problem. Yet the amount of work actually being done to understand and address these problems is shockingly small. Interest in organizing a field of cyber policy analysis is palpable and widespread, but it remains latent and diffuse, with few concrete actions having been taken to get things going.

These proposed grants constitute the first serious step in that direction—a big one, whose effects could be profound. Just by themselves, the three initiatives will represent an enormous upsurge in the amount of activity dedicated to cyber policy. Nothing like this has been done anywhere, and doing it at some of the world's top universities offers reasonable assurance of quality. As such, we will be establishing three strong centers of excellence—each having committed to keep at this work for the long haul—to which we and other new donors can make grants. For Hewlett, creating these three centers will enable us to put our remaining funds to other uses, giving us room to begin strengthening other kinds of institutions and experimenting with other kinds of activities. For other funders, the university initiatives will provide a place to

begin grantmaking, offering them an opportunity that does not presently exist to test the field and gain experience.

We also regard it as important to our goals that the three universities have different strengths and that their different approaches reflect those strengths: Berkeley using the iSchool, Stanford acting with a strong awareness of startup culture, and MIT capitalizing on its experience building technology platforms, and so forth. This diversity of capabilities and approaches should lead the universities to produce different but related work that will attract a broader range of scholars, practitioners, technology experts, journalists, and others to engage.

But the importance of these grants extends beyond what the universities themselves do directly. There are, for example, the longer term benefits that flow from teaching and training. Berkeley, Stanford, and MIT are among the world's foremost institutions in educating and placing scholars at other universities and training practitioners and leaders to work in government, business, and civil society. Once the new programs are up and running, we can expect a steady stream of scholars and practitioners to begin seeding other institutions. Nor are other universities likely just to relinquish the field to these three. Rather, as noted in the introduction, the mere announcement of something on this scale will invite the kind of interest and attention that attracts matching efforts.

This is what we mean when we say these grants can jumpstart the development of a cyber policy field, potentially proving to be as important in their way as prior grants we made that similarly launched other fields (like the OpenCourseWare grant we and Mellon made jointly to MIT, which created the OER field).

On the flip side, the main risk associated with these grants is that we achieve less than we want. Any number of things we hope the grants will generate might not come to fruition or might happen to a lesser extent than we expect: faculty from different disciplines might not choose to work together; the universities could fail successfully to engage enough faculty, students, external stakeholders, or donors; the ambitious research agendas could fail to gel; other universities, think tanks, and NGOs might not be prompted to develop their own cyber policy programs; new funders may not enter the field; and the like.

Risks of this nature are inherent in any venture, and our conversations with university leadership and faculty, as well as others in the field, lead us to estimate them as low. There are, nevertheless, two potential vulnerabilities worth highlighting in particular. First, while good leadership may not be sufficient for success, it is necessary, and there are possible concerns at all three universities.

As noted above, we explored these issues carefully and believe the leadership is more than capable and up to the task. We nevertheless made our concerns in this regard clear to the presidents of the universities and have their promises to watch this carefully and act if leadership falters. We plan to remain in close contact with all three institutions ourselves as further insurance.

Second, launching our Initiative with three big grants to universities could make us appear insular, by which I mean too "ivory tower" and academic in dealing with problems that are profoundly practical. This risk is to some extent mitigated by the fact that these particular universities all have strong records and reputations for engaging with actors outside the academy, especially when it comes to problems like those addressed by the Cyber Initiative. It will, nevertheless, be important for us to begin reaching out to actors outside the academy, something we are already planning to do.

Such risks notwithstanding, and we do not mean to minimize them, the conditions surrounding these grants are promising and, starting out at least, they seem primed for success.

IV. Conclusion

The goal of the Cyber Initiative is to launch a new field, and we believe this kind of frankly audacious gesture—simultaneously introducing substantial efforts at three universities with global reach and reputations—can be effective in doing so. Much additional work will still remain to be done. Universities are a critical element in our strategy to build a field of cyber policy analysis, both for the research they do and for their role in training scholars and practitioners. They are not, however, the whole story. We need to spread the word to other universities, develop something similar in the think tank world, find ways to reach relevant audiences (hackers, technology geeks, and the like) that do not typically engage with universities and think tanks, extend the field outside the United States, make sure the research produced is seen and used by policy makers, and bring other funders into the field. That's a lot of work, but these special grants offer us a way to make it all easier—generating a sense that the field exists, that it is important, and that supporting this sort of work can make a difference.