CENTER FOR LONG-TERM CYBERSECURITY

Cybersecurity Policy Ideas for a New Presidency

NOVEMBER 2016

INTRODUCTION

In two months, a new President will take office. That President will face the most expansive cybersecurity agenda in our nation's history. Attacks on well-known companies, political organizations, and government agencies over the last year pose a fundamental question: can *anyone* really be confident in online security? If the answer is no, foundational elements of our economy and our society are at real risk. Because a loss of confidence could be nearly as damaging, the new administration cannot afford to wait. It will need to act quickly and decisively on cybersecurity as a major executive priority. And that administration needs new ideas to inspire new successes.

This brief brochure reviews ideas we hope the incoming Trump Administration will consider as it develops a new cybersecurity agenda. We lay out options and programs—some simple, some less so—that the President should consider at each step in his first term.

You may be wondering why our organization—the Center for Long-Term Cybersecurity—would want to weigh in on these issues. We believe we have to. One way to move toward a better long-term cybersecurity future is to take meaningful short-term steps today. Our goal here is not simply to make progress against today's problems; it is to build the future, starting now.

We aim to be purposefully provocative. There are plenty of good ideas already on the table. The government will likely create commissions and the like to study problems, and that is all to the good. But the new administration also needs to offer new initiatives, including some not already common in the public domain, and some that are executable without a comprehensive review. Perspectives from Silicon Valley are perfectly positioned to spark such innovation.

The new administration has an important opportunity to change the way Americans think about cybersecurity. Most Americans today see cybersecurity as a technical problem that sits down the list of national priorities. We believe cybersecurity needs to be thought of as an existential risk to core American interests and values, rising close to the level of major armed conflict and climate change. That kind of profound shift in thinking is what the United States needs to make real progress on maintaining the promise of digital technology to improve our country in the long run.

WHAT SHOULD THE PRESIDENT DO

in the first **10** days?

Policy Recommendation #1: A New Declarative Deterrence

Our new administration has said that it is willing to challenge orthodoxies in foreign affairs; it hopes to set new ground rules and confront issues that past administrations have been reluctant to touch. As always, 'shaking up the status quo' presents risks as well as opportunities. We offer the following ideas in the spirit of focusing on the latter.

The new administration has an opportunity to set some new norms in nation-state cybersecurity behavior. Cyberattacks were unquestionably salient during the campaign, and so people are paying close attention. Part of the debate will be about 'active defense', both within the U.S. government and in the private sector.

Some may believe that it will be the instinct of the Trump Administration to 'hit back' harder against cyber-adversaries, particularly of the nation state variety. If true, the new President has a distinct opportunity to set the terms on which we believe norms of restraint should operate, as well as some notional boundaries to serve the long term interests of the United States.

Action is essential to achieve this goal. Norms are not made principally by talking about them, or by waiting for them to 'emerge' through some undefined process of diplomatic coalescence. Norms are made through highly visible action—and restraint of action— that is justified in clear and compelling ways at particularly salient moments in time. Now is the time to start the process of norm development in the active defense space.

What norms would we like to see emerge with regard to active defense? Two examples are:

- 'Privatized' active defense is an extraordinarily risky place to be. Others would benefit more than we would from a world where the shackles are off. The United States, in contrast, would benefit from a norm that 'states are responsible for attacks launched from their territory'. Such a norm does not mean that private active defense can't be deployed at times; a limited freedom, for a cabined window of time, against a cabined adversary, would vastly increase U.S. capabilities to respond. But that decision should be made in coordination with the government.
- Electoral systems are critical infrastructure, both here and abroad. The new administration should understand this better than most. It could draw a bright line by saying that 'the United States will not use its cyber-capabilities to intervene in the electoral processes of other countries . . . and will respond strongly should other governments attempt to influence ours'.

To start this process, the new President should make a public statement that the administration will respect these norms going forward. As with all deterrence policies, whether to undertake any particular action in response to an adversary's action is an entirely separate question. But making a declarative public statement has the potential to bolster deterrence, broadening the range of punishments against which adversaries would have to calculate. It will also send a powerful signal to the American public about the new centrality of cybersecurity to U.S. national security.

Policy Recommendations #2, #3, and #4: Grow Public Awareness, Forgive Loans for New Cyber Professionals . . . And Build an Incubator To Solve Tough Government Problems

A common theme around cybersecurity that crosses everyone we talk to—from cybersecurity experts to government officials to start-ups in Silicon Valley to major companies in New York and beyond—is that there is a shortage of human capital. The United States does not have enough professionals working in cybersecurity. Here is an area where jobs have been created—but there aren't enough qualified Americans to fill them.

We believe the cybersecurity workforce needs to operate on a pyramid structure. At the base of the pyramid are individuals who need a competent enough understanding of the basic technologies to be able to make informed corporate and government policy decisions. Boot camps and other educational opportunities/ trainings are the current preferred solution for getting non-technical decisionmakers up to speed. But these programs won't scale either quickly or broadly enough.

At the top of the pyramid, we need more PhDs—research professionals with the advanced technical skills required to design new systems that are less vulnerable to attack. We need to encourage new and more diverse groups to gain those high level skills, and provide meaningful opportunities for them to work on tough government problems.

We propose a three-pronged approach to cybersecurity education and advancement.

1. ***Grow The Base: Make Cybersecurity The Next Seatbelt.*** With increasingly universal access to the internet comes increasing need for individuals to be more knowledgeable about their digital security. Given the breadth of its impact, we believe that cybersecurity should be the next great public safety measure. We need our education system to treat cybersecurity as a fundamental part of computer literacy, in the same way that coding is becoming a norm. Following on from similar campaigns with bipartisan support (think seat belts and anti-smoking), the new administration could launch a public education campaign to prepare current and future generations for a world in which the internet is fully woven into the fabric of every American life.

> We need our education system to view cybersecurity as a fundamental part of computer literacy, in the same way that coding is becoming a norm.

2 ***Grow The Top: Forgive Loans and Open New Channels.*** Our universities aren't creating the number of top cybersecurity professionals needed by our government and companies. We should forgive (or at least defer) student loans for cybersecurity professionals. And we should open new channels—special cybersecurity visas for the foreign born, and online education for everyone—to make entering this field more viable no matter where you live. If a talented cybersecurity research professional wants to work in the United States, we should make that possible, and manage the risks accordingly.

3 ***Help Our Government: Establish a Cyber Workforce Incubator.*** Government is facing myriad cybersecurity challenges, and does not currently have the resources to solve them. Women and men across the West Coast have cutting-edge cybersecurity skills and technical knowledge, but lack viable, short-term opportunity to place their talents in the service of national security. Many do not wish to move back East. Many do not want to leave the West Coast work culture. Many still are not interested in holding a government job. And those who do opt to work in government often lose the up-to-date technical knowledge that made them so valuable in the first place. Our Executive Branch must develop new ways to bring the private sector's most innovative technologists into national service, while also permitting that talent to stay connected to private sector cyber innovation. The next President could improve cybersecurity knowledge flow and circulation by creating a new, nimble cyber incubator, allowing the West Coast's best technologists to work on national security challenges without giving up their work cultures and networks. With streamlined security clearances, cybersecurity professionals could be seconded to a new Valley-based organization for one to two year stints and work on the most important national security challenges, before returning to the private sector refreshed and inspired.

Cybersecurity is a unique space where our job creation and national security needs are aligned. President-elect Trump understands how a strong workforce drives business. By exerting early leadership in these areas, he can make a real difference in the cybersecurity talent pipeline.

Policy Recommendation #5: Create CARPA: The Cyber Advanced Research Projects Agency

Innovation will be at the core of any long term cybersecurity agenda, and so will research at universities like ours. But to really accelerate developments and harness new knowledge, we need much more investment in this space—both to fund research projects and to signal to society that cybersecurity is the new existential challenge for this generation to confront.

For this reason, we propose a new institution: CARPA, the Cyber Advanced Research Projects Agency. This new agency could aggregate existing government and DARPA cyber initiatives and focus specifically on innovating in a field that is increasingly critical to civilian as well as military life.

Why create a new institution, rather than fold it into DARPA? There is one simple reason: cybersecurity is not just about the defense establishment. Cybersecurity is about innovative technologies improving consumers' lives; it's about intellectual property and legal regimes; it's about small businesses that need security to enable their systems; and it's about human interactions that are increasingly taking place on evolving social media platforms. If we limit the scope of cybersecurity to offensive and defensive capabilities, we are missing a big piece of the puzzle.

There is precedent for spinning off programming initially managed by DARPA to specialized agencies. Some of DARPA's earliest projects focused on advancing space exploration technologies for the space race. In 1958, the Eisenhower Administration recognized the growing importance of space exploration beyond its military function, and Eisenhower signed the National Aeronautics and Space Act—establishing NASA.

Why can we not leave this work to the private sector? There is a simple answer here too. Digital security is too important. The future of our society is at stake, as artificial intelligence and machine learning proliferate, as the Internet of Things connects more of our devices, and as we move ever more of our day-to-day lives online. We need government, the private sector, and researchers all working together in this space. A significant institutional move will be required to signal and support a much higher level of attention, investment, and collaboration.

> Cybersecurity is the new existential challenge for this generation to confront.

CONCLUSION

If there is one thing we hope this brochure highlights, it is that America's existing cybersecurity toolbox is not adequate. The next President needs a longer list of options on the table, a list generated even in advance of inauguration, from which some complex choices will be made. We hope that the ideas generated here will make those choices both more expansive and more urgent. Many others—for instance, using the Internet of Things to support the new administration's call to improve national infrastructure—should also be put on the table.

The ideas we've offered likely look and feel different than those coming out of a traditional D.C. think tank. This is purposefully so. Silicon Valley believes in the value of unconventional options. Many of those options seemed crazy, risky, or improbable at first, but seem inspiring today. Many others fail—but improve our knowledge of what works and what doesn't in the process.

The most important message we want to send is this: to build a robust and successful cybersecurity agenda, our next President will need to figure out how better to use both the technologies and the processes that Silicon Valley creates. President Obama started a trend by bringing a lot of Valley alums to Washington, but only a select cohort will be willing to leave comfortable California for the Beltway. The next logical step—to bring D.C. to the Valley—has to be the long-term solution. Organizations like DIUX and In-Q-Tel have begun this process generally, and cyber-specific institutions are the next logical step.

We are passionate about and interested in playing a role in this process. Please reach out and engage with us, whether you agree or disagree with our ideas. It is through such collaboration that we can inspire a better cybersecurity future together.[1]

1 CLTC would like to thank Jesse Goldhammer, Jonathan Reiber, Chuck Kapelke, and Kristin Lin for their assistance in developing some of the ideas in this pamphlet, and Jacqueline Jones Design for brochure design and production.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley