NATIONAL
PREPAREDNESS
LEADERSHIP
INITIATIVE

National Leadership Dialogue on Cyber Security: Key Themes and Recommendations

Compiled by
Leonard J. Marcus
Ronald L. Banks
Eric J. McNulty
Richard Serino
Lisa B. Flynn

A collaboration between the USAF Cyber College and the National Preparedness Leadership Initiative

December 2, 2016

HARVARD T.H. CHAN
SCHOOL OF PUBLIC HEALTH

HARVARD Kennedy School
Center for Public
LEADERSHIP

National Preparedness Leadership Initiative

A Joint Program of the Division of Policy Translation and Leadership Development, Harvard T.H. Chan School of Public Health and the Center of Public Leadership at the Harvard Kennedy School of Government

This paper is distributed for informational and educational purposes only. No citation, quotation, duplication, or distribution without the expressed written permission of the authors. The authors wish to thank Jennifer Grimes for her assistance reviewing this paper.

National Preparedness Leadership Initiative
Harvard School of Public Health
http://npli.sph.harvard.edu
P.O. Box 381488, Cambridge, MA 02238-1488
617-496-0867

INTRODUCTION

The quandaries of cyber security have many sides. It is a technical problem that requires technical solutions. It is an economic problem imposing extraordinary costs on businesses. It is a security problem exposing to risk classified government information as well as valuable corporate and personal information. Cyber-attacks present a threat to the critical infrastructure and thereby could cripple normal social functioning. Ambiguities in jurisdictional boundaries, gaps in doctrine, unclear designations of accountability, and divergent definitions of threat thresholds impose obstacles to innovation and development of new technology. Cyber security is all this and more. It is now among the most complex and vexing problems facing government and corporate leaders.

Government, private, non-profit, and academic stakeholders representing different angles of this vast cyber security puzzle naturally posture on the side that most directly affects them, as would be expected. Likewise, given the unrelenting nature of the cyber security threat, they adopt a stance that limits their exposure and responsibility for mounting effective defensive and offensive remedies. Given the involvement of state actors and cyber criminals, the private sector expects the Federal government to play a protective intermediary role. Given that the cyber infrastructure is largely owned and operated by the private sector, government expects the private sector to protect its assets and operations. Confronting malicious cyber activity is neither a simple nor linear task. Among the most frequent observations heard in the two-year run up to this dialogue: too much time is spent admiring the problem or developing patchwork remedies that fail to address root causes. It is a multi-dimensional challenge requiring multi-dimensional thinking and action.

Given this complexity and array of perspectives, it is informative to view the problem from a “whole of cyber security” perspective. What is the benefit in looking at the whole? The network structure of the threats and potential solutions come into sharper view. Connections and interdependencies become more apparent. Otherwise elusive options and opportunities are explored. Leaders across the cyber security enterprise are best able to make a crucial conceptual leap when they view the problem together from this wider cyber security perspective.

To test this premise, the United States Air Force Air University’s Cyber College collaborated with the National Preparedness Leadership Initiative (NPLI), a joint program of the Harvard T.H. Chan School of Public Health and the Harvard Kennedy School of Government, to convene a meeting of key leaders across the cyber security enterprise. The one-day “National Leadership Dialogue on Cyber Security” convened at the Cambridge campus of Harvard University on August 2, 2016. The meeting built upon a two-year study into improving collaborative public-private cyber security strategy led by NPLI executive education participants. The dialogue was designed to forge new cross-sector connections and provoke fresh thinking regarding the defense of U.S. critical infrastructure from cyber-enabled malicious activity. The meeting included 47 participants: 22 from the private sector, including financial communications and technology companies; 17 from the federal government, including the Department of Defense, Department of Homeland Security, Department of the Treasury, Department of Justice and National Security Agency; 3 from the non-profit sector; and 5 academics.

The dialogue followed a simple non-attribution ground rule. The discussion was facilitated by Harvard NPLI faculty members. To collect perspectives from all participants, the Poll Everywhere voting tool was used throughout the meeting. Polling responses were reported using both percentages and key words. Each Poll Everywhere question generated dialogue that built upon the responses and their implications. What follows are the unattributed comments from the day and general themes arising from dialogue among those national leaders, along with their recommendations for action for the incoming Presidential administration.

LEADERSHIP: THE HUMAN FACTORS

Framing the Problem

The opening questions asked the participants about the preparedness of the current cyber security system. Public and private sector leaders responded together. 76% replied that the system ranged from completely not ready to not very close to ready, while 24% said that it was close or very close. When asked about how well prepared the system is to diminish or reverse the trajectory of cyber threats and consequences, 84% said poor or not very well prepared. Asked to submit one word suggestions to improve system readiness, participants' responses centered on collaboration, communication, responsibility, and leadership.

There was a consensus among participants that leadership, not technology, is the limiting factor in addressing the nation's most significant cyber security challenges. There is an assumption of a common vision to address cyber security, "which we do not have," as one participant declared.. Another stated there is "too much focus on technology," while another highlighted a landscape too often "…viewed in an adversarial context, not at people and unified interests. There is a lack of consideration of strategy, outcomes, and intent." A fourth commented, "Starting at the human element of how we are all affected as a society is a good place to start." It was suggested that leaders should look beyond tangible losses to the effect on the public psyche: "the American system [of commerce] relies on trust," while difficulties in attribution of malicious behavior and the virtual nature of the digital space mean that cyber-attacks are particularly damaging to trust in that system. Echoing this, another participant commented that cyber-defense is as much about protecting American values as it is about securing assets.

Focusing on a Unifying Vision

Turning to leadership, one participant noted that just as technology is not the most significant challenge, “policy is not leadership.” Policy development is necessary but not sufficient to solve the problem. A participant called for a bold vision with a quantifiable goal, a strategy to get there, and accountability for results. Another echoed that an audacious goal and timeline are needed to push people out of their comfort zones, catalyze fresh thinking about how to balance privacy and security, and stimulate investment in innovation. One example of big thinking offered was to “make cyberspace as safe as physical space.”

The theme of leadership evolved later in the day into a discussion of a cyber “moon shot” focused on “making a serious dent” in the $440 billion in losses by private organizations to organized crime. The stated ambition was to reduce 80% of this cyber-crime within two years. It was noted that for this segment of malicious cyber activity, there is basic agreement on the threat, consequences, and motivations of the malicious actors, which would make system collaboration easier. Additionally, jurisdictional lanes are relatively clear. By way of illustration, a project underway at the National Cyber-Forensics and Training Center could provide guidance on how to bring together business, government, and academia to achieve stated objectives. Such an initiative would require unity of effort across sectors including educating the general public. “Basic cyber hygiene, both personal and organizational, would take care of a good amount of the low-level criminal activity,” one person noted. In a later poll, participants agreed that both government and business need to do a better job of securing their own environments.

Within such a unified endeavor, each sector would still have distinct roles to play. Polled as to what federal government should do to improve the current national cyber security system, the participants’ most common responses were, “lead,” “listen,” “communicate,” “prioritize,” “set standards,” and “provide incentives.” Asked a similar question about the private sector, participants responded, “share,” “innovate,” “get ahead of the tech curve,” “invest,” “participate,” and “lead.”

Moving to Whole of Nation Cyber security

Participants expressed the belief that an improved effort against organized cyber-crime could be a cornerstone for a “whole of nation” approach to cyber security. This would address the threat directly, and in the process engage a broad swath of those potentially affected.

Additionally, an initial focus on organized crime would lessen the distractions inherent in thornier and more complex cyber threats, such as attacks by state actors or those directed at the critical infrastructure, while still strengthening essential relationships. Reducing organized cyber-crime would “improve the signal-to-noise ratio” in the threat and response environment, making it easier to dedicate the best talent and right resources to counter the most significant threats from state and/or state sponsored threats to national physical and economic security. More importantly, the whole of nation approach would focus on imposing tangible consequences on malicious cyber actors whose current cost/benefit calculus weighs heavily in their favor.

A true whole of nation approach requires embracing complexity. The principles of swarm leadership (see below) can apply to help bring together the many stakeholders whose participation is necessary in finding solutions. Complexity refers to the dynamic relationships among all participants in the larger cyber-system, including between both good and bad actors. Whole of nation requires moving beyond worrying just about “my piece” and looking at the system as a whole, recognizing how different yet legitimate motivations, incentives, impediments shape behavior. According to one relevant insight, “every system is designed to get the results it gets.” Based on participants’ observations and contributions, the current system is designed to encourage dis-connectivity. This is due to narrow perspectives on threats and remedies; lack of clarity about the roles and responsibilities of different organizations, agencies and sectors; and information sharing that is fragmented, late-to-need, and not strategic.

SWARM LEADERSHIP

Derived from the NPLI faculty’s study of leaders in the Boston Marathon bombing response, swarm leadership describes leader behaviors and leadership conditions that promote robust coordination and collaboration across organizational and jurisdictional boundaries when no one organization is in charge of the overall operation. The five principles of swarm leadership are:

1. Unity of Mission
2. Generosity of Spirit and Action
3. Staying in One’s Lane
4. No Ego, No Blame
5. A Foundation of Trust-based Relationships

For more on swarm leadership, download this white paper.

One participant used a sports analogy to describe the need for a shift in the system's paradigm: "this is not two teams on a field wearing different colored uniforms. Anyone in the stadium could be an asset or a threat. A linear playbook will never counter this threat." Instead it will take active collaboration and coordination across sectors, articulated during the discussion in terms of swarm leadership.

A constructive conversation arose about changing the risk/reward calculations of the malicious actors. "Vulnerabilities will always exist," said one person. "Our goal should be to reduce them while improving response capability and resilience in the system." Another explained, "We are dealing with nimble, adaptive enemies. We have to find a way to work with ambiguity. How can we maneuver and evolve cohesively?"

Again, trust emerged as a central issue. Private sector participants raised a persistent risk: voluntarily sharing information could potentially have negative regulatory impact on their business interests, breeding distrust between private entities and public agencies. Several participants commented that there is a general distrust of what is shared across sectors because it is perceived to be old, incomplete, or overly sanitized. There is a feeling that the "real" information is being horded and only shared selectively.

In relation to the trust issue, one participant articulated the need to move beyond the "I know a guy network," whereby people place greater confidence in their informal networks than in the formal relationships. This participant added, "It exists because people feel comfortable sharing with people like them, in the same industry with the same problems. Ultimately, we must move toward public sharing and hold people accountable. If you aren't sharing publicly, you are part of the problem." While disagreement persists on the question of information sharing, participants agreed that sharing should be as close to real time as possible while protecting proprietary records and personal privacy.

A point of significant discussion surrounded the job of defining the scope of the cyber security mission, from the perspective of each entity and each sector, along with how they together might address the question. Disagreement centered on the question of "who owns the problem?" Multiple government agencies play a role and each looks at the national cyber security question differently. There is contextual variability in attacks. "Who is the perpetrator?" and "who are the targets?" are important variables to examine. A participant pointed out, "It is not easy to decide who makes a call when there is an attack on private industry. Freedom of response rests at a lower threshold" when it is not a state actor acting against a state target.

Transitioning toward a whole of nation cyber security strategy requires a combination of offensive and defensive tactics. One person said, "Always being in defensive mode is unacceptable in the long term." This continued into a robust discussion of how far upstream one might fight these battles. Another noted, “We should not always be focusing on what to do when the incident has already happened. By the time the alert comes out, we are breached. We’ve failed.” Several participants suggested that by working together, public and private entities can push some of the response activity ‘left of boom’ through preemptive action. For example, currently a private entity such as an internet service provider may coordinate with the Department of Justice when the FBI or Secret Service decides to disrupt at botnet organization. It was argued, however, that more could be done by looking beyond standard investigatory dismantling to see how the malicious actors are operating in the delivery infrastructure. With that, it is possible to discern what legal action might “take out” their infrastructure before an attack occurs.

It was recommended that all stakeholders work together to define “unacceptable losses” (as articulated by Young and Leveson of M.I.T.) as a way to help determine where a whole of nation strategy is most urgently needed.

The Need for Speed

Speed was a recurring theme throughout the day, identified as a hallmark of an agile and resilient system. Specifically, speed was deemed essential in:

- Identifying threats;
- Sharing and collaboration;
- Adapting defenses and offenses;
- Coordinating response and recovery. It was noted that when an agile, highly adaptive swarm confronts a rigid, cumbersome bureaucracy, the swarm will always win. The “good guys” must evolve as quickly—or even more quickly—than their adversaries in order to create a truly secure cyber environment;
- Changing the economics of crime. The more rapidly and effectively target organizations perceive, prepare for and respond a threat, the lower the criminal success rate, and thus the lower return on investment of time and resources by malicious actors.

It was suggested that common metrics to assess speed—what is acceptable, what is best-in-class—could rally different entities to find new ways to solve universal challenges in place of battling over turf. There would be less incentive to reflexively say, “Don’t worry, we’ve got it,” and more encouragement to collaborate with other entities to continuously improve system performance.

One person noted that when the federal government establishes new priorities or sets upgraded standards, it unleashes a substantial private investment response, with creative energy to develop marketable products and services to achieve the new objectives. This phenomenon, combined with funding for basic research, will speed innovation.

The Department of Justice also has sponsored pilot projects through which private industry funds and develops new products and services that can later be authorized for use by the government, as long as they conform to pre-established regulatory and legal standards. A participant opined, “This could be a general model for dynamic collaboration between the Federal government and the private sector to proactively identify potentially crippling attacks and propose solutions.” It could be an avenue to speed response and recovery.

There was a robust discussion about the need for a clear map of the eco-system in order to advance collaboration and information sharing. The idea was to build upon Presidential Policy Directive (PPD) 20, 21, and 41 by identifying gaps in strategy, organizational structure, and response options. For example, recently released PPD-41 neither mentions local and state governments nor the Department of Defense. This sort of gap analysis should inform the development of policies, protocols, and plans to more holistically include connectivity of action within the system. With a consistent eco-system perspective and strategy, the private sector and all levels of government will integrate better their understanding of threats to the system and actions in order to alleviate the attendant risks.

Finding the Right Metaphor: Words Matter

It became clear throughout the day that it will be important to frame ongoing conversations with the right metaphor. The frame of reference is powerful in setting assumptions and expectations. One aspect of the struggle in aligning interests and activities lies in the disparate mental models that stakeholders bring to the table. A war metaphor, for example, is one in which the government is clearly in the lead with expectations of a definitive victory. The private sector plays a supporting role. By contrast, a law enforcement metaphor sets different expectations: crime is never fully eliminated but mitigated and controlled. A different set of actors is engaged in pursuing and prosecuting malicious actors.

Unfortunately, neither metaphor adequately addresses the current cyber threat environment. The “war” metaphor establishes a very high threshold for federal government action, while the “law enforcement” metaphor cannot impose widespread meaningful consequences on malicious cyber actors. Furthermore, neither metaphor acknowledges the reality that private corporations bear much of the obligation to respond along with most of the risk.

Several other interesting metaphors emerged throughout the day:

A Cyber Moonshot

The “moonshot” mentioned above suggests an ambitious, aspirational goal involving multiple stakeholders. It is a pro-active approach to a clearly defined, meaningful objective with a shortened time horizon. The evolution of space exploration spurred greater participation by the private sector in lead roles. A similar goal should be set by the new administration that galvanizes national, unified action to appreciably change the cyber status quo. To emphasize the “moonshot” is to bring private and government entities together in a synergistic way to impose consequences on the adversary through both virtual and non-virtual means.

The Public Health Model

An “infectious disease” metaphor also was raised. The emphasis here is on rapidly detecting and containing the outbreak: punishing bad actors by limiting their impact is as important as traditional prosecution. This approach acknowledges the difficulties of attribution and, if attribution is achieved, the further difficulties of apprehending and prosecuting perpetrators when they reside outside of the U.S. In a public health response, “everyone knows who to call, the CDC (Centers for Disease Control and Prevention)” and government, big pharma, and other entities cooperate without immediate concern regarding “how to make a dollar.” Instead, the priority is “addressing the threat in a timely manner.”

The Natural Disaster Model

Playing off the infectious disease analogy, another participant suggested thinking about cyber as we do natural disaster response. FEMA (Federal Emergency Management Agency) serves as a coordinator of federal participants and as single point-of-contact for private sector entities. As explained by a participant, “There are so many touchpoints in government that industry uses…There is only one counterterrorism center but, for cyber, there are a number of coordinating agencies. It’s hard to change culture over a broad range of entities.” Another agreed, saying, “FEMA is a coordinator. Cyber needs a coordinator to deal with the lack of defined roles and responsibilities.”

Related to this model, Joint Interagency Task Force (JIATF) South was offered as a possible guide. To achieve its anti-drug mission, JIATF South integrates agencies that own a piece of the mission into a common operating environment. This collaborative framework encourages the very relationship building and information sharing required to address complex problems. JIATF-South, under the purview of the Commander of USSOUTHCOM, is tasked to stem the flow of narcotics into the U.S. through the

Caribbean and Gulf of Mexico regions. This task force exemplifies an ongoing interagency effort to conduct cooperative operations. A measure of the task force's success is found in its well-integrated interagency operations, which utilize the existing authorities of each participating U.S. government department and agency.

FEMA TRANSFORMATION

Richard Serino, former deputy administrator and now distinguished visiting fellow at the NPLI, shared the process of cultural transformation at FEMA as a way to inspire fresh thinking about cyber security. He discussed "three L's": language, linking, and listening.

Language: FEMA redefined the word "victim" to narrowly refer to those who die in a disaster. Everyone else affected is a "survivor." Serino noted that victims expect others to act for them while survivors expect to participate in response and recovery. Being intentional about language establishes a different set of expectations, thereby increasing system capacity and capability.

Linking: FEMA actively linked their efforts to those of volunteer organizations active in disasters (VOADs) and the private sector. Serino emphasized that FEMA is "never in charge." It is a support-and-coordination agency. Rather than ignoring or attempting to supplant the efforts of others, it sought out gaps to fill. "We stopped trying to do what others were doing well and instead looked to how we could help make them successful," said Serino. The result was less conflict and greater responsiveness to the needs of survivors and their communities.

Listening: When FEMA changed its orientation from declaring "here's what we're going to do" to asking survivors and other stakeholders, "What do you need?", the dynamic of the response transformed. There was less hostility to the Federal presence. Federal agencies achieved greater impact in their post-disaster activities. The system became more responsive, efficient, and effective.

The Open Seas Model

Open seas doctrine was offered as another analogy and possible model. One participant explained that the introduction of steam power brought tremendous growth in international shipping. “The state provided an environment with a certain sense of predictability and rules. Within this environment, businesses could make decisions. Pirates still existed but there was the concept of a regulatory regime, compliance, and attribution.” Further, it was noted that cyber is still a relatively new marketplace and, as with any new marketplace, the state has a role in generating certainty in governance to appropriately stimulate robust economic activity and innovation, but also a role in the protection of those who choose to operate in the marketplace.

The Road Safety Model

The final metaphor that gained traction was road safety. The public and private sectors have worked together to continually reduce traffic deaths through improved road and vehicle design, consistent signage and traffic rules, and extensive education. There are regulated minimum standards, still automakers also can compete to offer additional safety features that have market appeal. While the system is not perfect and there is still much to be done, this model has encouraged routine and manageable safe driving behaviors for most people. By contrast, cyber security requires the public and corporate IT managers to employ increasingly cumbersome defensive measures, including complex passwords and two-factor authentication. It was noted that the harder it becomes to comply with security measures, the more likely are people to become frustrated and seek ways to avoid the most secure applications, services and procedures. Several participants argued that it is time to think “beyond passwords” and to catalyze innovations that will embed greater security into the overall system.

None of the above metaphors fully captures the complexities of the cyber environment. Each, however, may be deployed successfully to advance the dialogue about different conceptualizations, strategies and priorities in the cyber arena. Clarifying the dominant metaphor also can reduce misperceptions, unnecessary conflict, and the resultant resistance to collaboration.

CONCLUSION

As the day-long dialogue reached its conclusion, a participant shared the quote from President John F. Kennedy’s "Moonshot" speech to Congress on May 25, 1961:

"I believe we possess all the resources and talents necessary. But the facts of the matter are that we have never made the national decisions or marshaled the national resources required for such leadership. We have never specified long-range goals on an urgent time schedule, or managed our resources and our time so as to insure their fulfillment."

There was significant enthusiasm for this proposal of a wide-sweeping “Cyber Moon Shot.” The analysis of the overall discussion and priorities addressed during the day-long dialogue pointed to three key themes: 1) human factors supersede technology on overall questions of cyber security and the pursuit of strategies to meet the threat; 2) strategic government-private sector dialogue and partnership adds significant value to the fight; 3) leaders must transform thinking surrounding existing assumptions about the problem, potential solutions, and frameworks in order to overcome the cyber security threat.

Ten key recommendations emerged:

1. **Mission: Declare a Cyber Moonshot.** Markedly degrade organized cyber-crime, which constitutes 80% of malicious cyber activity, through an energized and elevated government/private sector partnership that appreciably imposes costs and other consequences on malicious cyber actors.

2. **Timeline: There is rallying value in speed.** Within two years, ensure the defense and vitality of US critical infrastructure and to prevent a significant cyber incident. Stimulate innovation and challenge norms through strategic stimuli that motivate quick and effective solutions.

3. **Metrics: An ambitious goal.** Cut in half the $440 billion drain on global economies by transnational organized crime (TOC). Significantly raise the cost of business and risks to malicious cyber actors.

4. **Leadership: Focus on people, not simply technology.** Build collaboration at the highest levels of government, across key agencies with relevant authorities and in partnership with the private sector. Organize around a compelling, unifying principle and mission. Build a foundation of trusted relationships to combat transnational organized cyber-crime.

5. **Coordination: Design connectivity of effort.** Build upon PPD-41, 20, 21, and EO 13636, to integrate systematically the private sector into “left of boom,” proactive interdiction. Close the gap between the rising tide of malicious cyber activity and response activities. Anticipate challenge to construct effective strategies and tactics to thwart it.

6. **Strategy: Link international organizations and multi-national corporate entities**. Fortify the development of unified and aggressive laws in all participating countries and aggressively target cyber-crime organizations. The U.S. must lead and set the standard for norms and operations for the global community.

7. **Align Incentives: Fund and mandate government agencies and incentivize the private sector.** This is U.S. Government mission priority. Provide tax breaks and seed money to leverage the capabilities of the private sector and create innovative solutions to the cyber security threat.

8. **Bolster End User Capabilities: Educate and enroll the public.** Make the public a knowing partner in the fight against cyber-crime. Warn the public of the risks they face and make it easy and automatic for them to engage and respond. Encourage private sector investments in customer cyber safety.

9. **Transparency: Create a clear map of key players.** Chart the engagement, authority, accountability, responsibilities, and rapid information sharing across public and private sector stakeholders to advance the tenacity and resilience of the campaign.

10. **Next step: Campaign launch with the President alongside private sector leaders.** Declare the cyber moonshot as a shared government-private priority. Engage Congress and the incoming Administration with a theme, plan, and measurable objectives. The campaign must be viewed as a cooperative endeavor, with government and private leaders co-leading the initiative, and not as one of the government mandating private industry’s participation. Both side must “own” the problem and be indispensable leaders/partners in the campaign.

ACKNOWLEDGEMENTS

The National Preparedness Leadership Initiative (NPLI) extends its appreciation to Lt. Gen. Steven L. Kwast, Commander and President, Air University, Maxwell Air Force Base, Alabama, our co-host for the project, and the Air University for its support of this national dialogue.

We also would like to thank the following:

Col. (ret.) Ronald Banks of the U.S. Air Force. Col. Banks' NPLI meta-leadership project team launched the initial work seeking a pragmatic approach to strategy and policy to combat major cyber threats from state and state-sponsored actors. The NPLI Cyber Team set to establish a new strategy for defending U.S. critical infrastructure by overcoming current hurdles in partnership between government and private sectors, while also imposing consequences on malicious cyber actors. The team members were: Col. Banks, Anthony Bishop (USAA Insurance), Jason Jordan (Bank of America), Mark Butt (U.S. Coast Guard), Ashu Palta (Los Angeles Country, CA), James Anderson (U.S. Northcom), and Larico Harley (U.S. National Counterterrorism Center). This project and subsequent follow-on work ultimately led to this national dialogue on cyber security.

Col. Steven Luczyinski, Senior Military Advisor to the Office of the Secretary of Defense on cyber policy. Col. Luczyinski led another NPLI project team that addressed how electric utilities could best prepare for and mitigate cyber threats. He was active in maintaining the momentum toward this event.

Lisa Flynn, J.D., M.P.H. who was a note-taker for the event and is a co-author of this report.

Barlow Keener, J.D. was a note-taker for the event.

Frances Walsh was a note-taker for the event.