
REBOOT

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

LLNL-TR-435055 Q1242

Reboot

Defining Paths to Cyber Policy, Law, and Technology Solutions

March 25, 2010
San Francisco

This page intentionally left blank

Executive Summary

As numerous studies, reports, and public discussions have clearly articulated over the past several years, the threat and potential impact of cyberattacks against the United States is growing daily. Moreover, there is an increasing awareness and recognition that given the relative "lawless" nature of cyberspace—the "Wild West" analogy—governments must step up to the challenge of more closely partnering with the private sector, which ultimately owns, operates, and continues to develop the technologies and systems that comprise the network. This partnership must be genuine and built solidly on a trust relationship. At the federal level, the United States government must develop and nurture a security environment where all parties, to include individual citizens, understand and execute their roles and responsibilities in creating and maintaining a secure, functional, and interdependent communication network. Government has the responsibility, authority, and resources to establish parameters and incentivize secure behaviors before, during, and after some cyber "event." The private sector has the means and often the business drivers to ensure operational continuity of the nation's information networks. What is required is the motivation to more routinely work within industry sectors and more closely with government to organize comprehensive and robust solutions with reasonable expectations of protection from unreasonable exposure and liability that such cooperation currently exposes.

Lawrence Livermore National Laboratory and Georgetown University hosted this workshop with support from the Bipartisan Policy Center to further their collaboration in developing innovative solutions to current and future challenges in cyberspace. The workshop capitalized on the talent and experience of participants in the areas of policy, law, technology, and industry and leveraged the results of the recent government decision-making simulation "Cyber ShockWave," conducted by the Bipartisan Policy Center. While the general findings of the workshop were consistent with many expressed through recent studies and analyses, this study has identified several timely and novel recommendations for action.

- *Clear Priorities* are needed to effectively mobilize resources and evaluate threats to the integrity and stability of the cyber domain.
- *Anticipatory Measures* will help thwart attacks and prepare for recovery in the event of disruption or denial of service.
- *Legislative Action* will enable key players to act quickly and decisively with established roles and responsibilities in addition to adequate funding.
- *Technical Confidence* in defensive capabilities encourages those who protect the cyber domain to develop tools and procedures to limit the spread of malicious activity.
- *Education Efforts* ensure that current Internet users as well as future generations act responsibly to protect themselves and others from attack while fostering innovation in—and appreciation for—technological advancement.

Workshop participants were charged with going further than developing general observations and were asked to play the role of commissioners in the inevitable Special Commission that would follow a national-level cyber event. Comprising four panels, participants considered issues and specific recommendations for the following:

- Government and industry partnership for national-scale cyberattack.
- Building the policy and legal framework—understanding authorities and roles.
- Technical decision support and emergency response—how to improve the technical guidance.
- Recovery and communication—cleaning up the chaos.

Recommendations from the panels are useful for defining additional areas of policy, legal, and technical consideration, research, and development and can focus subsequent efforts of government, industry, and the academic and technical research community. Lawrence Livermore National Laboratory and Georgetown University are committed to pursuing a collaborative research program beginning with the results of "Reboot."

Introduction

The threat of cyberattacks against the United States is growing daily. Recent reports indicate that the number of Americans with Internet access is increasing while the federal government launches a new initiative to provide broadband capabilities to 90% of the United States in the next decade. Such connectivity will certainly improve the lives of millions of people, and it will also increase the size of the cybersecurity problem – more people, more information, and more systems will be at risk. To block incoming malware and the spread of botnets, among other perils, government and industry must work to develop effective defense mechanisms designed to protect cyberspace while maintaining freedom of information and privacy.

Given the history of major calls to action dating at least from the 1990s, recent efforts have focused more intensively on overcoming barriers to progress. Georgetown University has contributed most recently through three symposia, two organized by its Institute for Law, Science, and Global Security and cosponsored with Lawrence Livermore National Laboratory. The first event, in October 2009, was entitled "Integrating Disciplines: Cyber Security, Law and Policy" and held on Georgetown's campus, a location conducive to engaging a range of experts from the Washington, DC area. The event's discussions identified a sense of urgency for tackling the hard problems at the nexus of law, policy and technology for cybersecurity and a growing set of partners who are ready to find answers to many of the questions posed during the symposium. Next, providing a glimpse into the policy implications of a simulated cyberattack on American networks, the Bipartisan Policy Center's "Cyber ShockWave" identified gaps in the existing national security framework and demonstrated to the general public the demand for improvements in U.S. defense capabilities in cyberspace.

This report will highlight the findings of the most recent gathering. "Reboot," a workshop on policy, law and technology for cybersecurity, was co-hosted by Lawrence Livermore National Laboratory and Georgetown University in the San Francisco Bay Area on March 25, 2010. Engaging research and policy expertise, this workshop illuminated research needs as well as policy options and the potential interactions between research and policy. While useful contributions to the public debate in their own right, these inputs will inform specific next steps: production of a report, identification of potential research sponsors, proposals for future groups or presentations at other conferences, and other ways to advance research in these areas. The workshop reaffirmed Georgetown University's commitment to build a community of people, beginning with its collaboration with Lawrence Livermore, around cybersecurity to advance solutions that address this critical national need. This report aims to establish a research roadmap and further the national dialog in cybersecurity.

Laying the Foundation

To demonstrate the sense of urgency with which government and industry must address cybersecurity vulnerabilities, "Reboot" worked within a model established at the "Cyber ShockWave" event held in February 2010. The simulation, hosted by the Bipartisan Policy Center in Washington DC, demonstrated key areas of concern with regard to U.S. preparedness for a cyberattack. Participants in the most recent workshop were faced with the following scenario:

> *The U.S. has just suffered a devastating cyber attack on its communication and energy infrastructure. After several weeks of chaos much of the country is returning to a reasonable level of normal life but the impact on the economy and public confidence in technology and government will linger.*
>
> *Events of the past month have brought several issues into sharp focus:*
>
> - *While not fully depicted in the simulation, the first responders in a cyberattack would likely come from the telecommunication companies and the utilities. They were not prepared to deal with a crisis that rapidly grew beyond their typical scope. The transition between a private sector response and a national response depends on a public-private partnership focusing on this type of event.*
> - *The country needs a capability for rapid analysis and prediction of the evolution of such an attack. In the recent attack the government could not make any real assessment of how to stop the attack or of how far it would spread.*
> - *The legal and policy framework was entirely new territory. Even if there had been a recommended course of action, the authorities necessary to implement it were not clear.*
> - *The physical recovery took weeks and the recovery of confidence may take years. We have little capability for damage assessment and for planning rapid recovery.*

"Cyber ShockWave" presented a unique opportunity for policymakers, technologists, and industry to see, first-hand, the gaps in the current cybersecurity framework. Although any such simulation involves practical compromises, the active engagement of decision-makers in working through a scenario is a valuable complement to traditional scholarship and policy analyses.

The pervasiveness of cyberspace, its growing role in daily life, requires cybersecurity to be broken down into manageable sub-problems. The situation is complicated by the intersection of different communities and policy orientations – civilian and military components of government and business that supply and use information technology, and ordinary citizens engaged in private activity and in interactions with the government. Historically, these domains might be more easily separable, but at some level, all have a connection to a common body of technology. That situation complicates the identification, formulation, and implementation of rules (laws, regulations, organizational policies and procedures, etc.) and responses. What makes the early 2000s different from the early 1990s is the much greater presence of individuals in cyberspace, which means that the cybersecurity problem goes well beyond that of organizations in business, government, or the nonprofit sector. It is easy to argue that every

citizen must resolve to make his or her individual contributions to the defense of cyberspace. However, credible, practical planning for popular behavior greatly magnifies the challenge on the organizational front, where numerous reports indicate that progress has been underwhelming.

From a scientific standpoint, technologists face three basic challenges when it comes to defending cyberspace: (1) defining the current problem in clear terms, (2) developing models that adequately address the scale of the crisis, and (3) creating new capabilities for engineering and science that provide solutions to cybersecurity challenges. While each of these categories requires examination and analysis, work has already been started to meet the needs of today's vulnerabilities through academic study and applied research in the field.

Academics working on cybersecurity issues will first need to define the landscape within their field of study and then rebuild the defense mechanisms. This will require the establishment of a common vocabulary that can be applied to a variety of disciplines to construct a comprehensive analysis of weaknesses in the area of cybersecurity. Many have argued for a clean slate approach that will encourage creative solutions that both anticipate and detect threats to U.S. networks and also respond effectively through improved situational awareness. Such measures will require the hardening of existing components like intrusion detection systems as well as the development of new tools that address challenges in the increasing complexity the cyber domain.

Dr. George Cybenko of Dartmouth College suggested that a standard framework from national security could be particularly useful for thinking about cybersecurity: the OODA loop, which identifies and connects actions for observing, orienting, deciding, and acting. Cybenko suggested that researchers would benefit from this framework, which can motivate efforts to, for example, develop the capacity to monitor and act within milliseconds while limiting the number of potentially false positive reports. There are already efforts to increase the number of sensors placed on the network to observe Internet traffic and content. Such systems have already raised concerns about legality; even their use in government raises questions if they are applied to interactions between government officials and the public.

Industry leaders point to several key areas in which private companies can promote the United States as a leader in cybersecurity technology. Mr. Don Proctor of Cisco Systems observed that this generation of cybersecurity no longer focuses on toll fraud or cyber hacking, but rather on cyber crime in which the victim has changed from phone companies and big business to the average citizen. The forces that are driving such change are technology, economics and demographics—the forces that have been driving the diffusion of the Internet across U.S. society and across nations. Technology includes the proliferation of connected devices, which increasingly include consumer devices of various kinds, as well as the proliferation of wireless systems, enabling a more mobile workforce and fostering reliance on the shared platforms for computing and data storage sometimes referred to as cloud-based computing. Whether that cloud supports social networking or the activities of global businesses or multifaceted governments, a consequence of these trends is that securing a borderless network requires an in-depth, architectural approach by industry and government. A continued partnership between the public and private sectors will benefit not only supply-chain security and network safety, but also reduce the innovation gap by decreasing the amount of time it takes between product certifications and acquisition of new technology.

Protecting national assets and critical infrastructure involves analyzing how the United States can defend systems that are vital to commerce and other societal functions and yet are vulnerable to hackers and cyberattacks from governments as well as non-state actors, whether organized or acting as individuals. As the search continues for the technological elixir, the problem of cybersecurity may not be one of technology, but one of law and policy.

The United States lacks a coherent set of laws addressing cybersecurity, notwithstanding legislative activity dating at least to the mid-1980s. A number of executive orders conferring authority on various agencies exist to secure governmental computer systems and communications and to assist the private sector in securing vital sectors. The legal authorities that exist in some instances reflect a balance of concerns that may have worked better in the past, under different circumstances—although that is by no means agreed among stakeholders. For example, legal prohibitions against conducting electronic surveillance on computer activity may also inhibit efforts by law enforcement to trace a cyberattack back to its origin to find the source of the cyber intrusion. Advocates for different kinds of balances make different arguments about the adequacy and the impact of today's laws and policies.

From conversations and recommendations made throughout the workshop, a set of policy suggestions that address the roles of policy, technology, and industry are detailed in the next section.

Concrete Solutions

"Cyber ShockWave" Hot Wash Recap

Immediately following the "Cyber ShockWave" event in February, leaders from industry and academia took part in an analysis of the simulation and discussed how government actions may impact business as well as future study. Those individuals included Dr. Catherine Lotrionte of Georgetown University, Mr. Michael Barrett of PayPal, and Mr. Rick Roscitt of SMobile Systems. To best engage with the participants of this workshop, the aforementioned members of that group participated in a roundtable conversation about the lessons of "Cyber ShockWave" and answered a variety of questions.

Dr. Lotrionte first assessed many of the legal ambiguities that were highlighted as a result of "Cyber ShockWave." With the absence of a clear declaratory policy that defines roles and responsibilities in national security events, she said, the U.S. government will continue to lack sufficient means to successfully address its vulnerabilities. More specifically, Dr. Lotrionte discussed some of the flaws she found in the legal reasoning considered by members of the "Cyber ShockWave" simulation regarding presidential authority. She cited the *Steel Seizure* case in which the Supreme Court ruled that the president only had the power to assume control of private industry during times of national crisis where a clear foreign nexus was present. In the case of cyberattacks, she argued, the President would indeed have the authority to defend government networks even if that meant circumventing private industry.

Mr. Barrett followed up on this topic by mentioning some of his reservations regarding the simulation. Although the scenario that was used provided a good case study, it was an extreme example and did not take into account what industry leaders would do in a real cyberattack situation. Representatives from the Bipartisan Policy Center, who hosted "Cyber ShockWave," reminded the audience that the simulation had to start from somewhere and it was vital, according to some of those who created the simulation, not to expose too many of America's cyber vulnerabilities. If a real cyberattack were to occur, it was argued, many of the affected ISACs (Information Sharing and Analysis Centers) would be assembled to coordinate a response. Mr. Barrett followed up by saying that many major mobile phone providers, for example, are now reconsidering their terms of service in preparation for a potential attack. Going forward, he suggested that societies would require similar security frameworks as those used in road and air safety. He encouraged distinctions made between the responsibilities for government, individuals, and companies to address this concern.

Finally, Mr. Roscitt concluded the debrief by suggesting that the U.S. government is not currently postured to take adequate action to thwart cyberattacks. Given congressional authorities to regulate interstate commerce and presidential power to defend the United States, steps can be taken that would mitigate future threats through prevention programs. Many believe that a catastrophic cyberattack on U.S. networks is not essential to see more government action in this domain. However, industry leaders caution that federal regulations ought to do only what is needed to secure networks and not more, which could potentially stifle technological innovation or growth.

At the close of this segment of the workshop, participants were advised that a summary of "Cyber ShockWave" would be taking place in the late spring or summer of 2010 for congressional leaders and their staff to demonstrate the urgency for action in defending against

cyberattacks. The feedback provided to the Bipartisan Policy Center in the debrief described above will be factored into the new scenarios.

Common Themes

The breakout sessions were intended to play the role of the commissions that would have been established in the wake of a catastrophic cyberattack. The mission of each group was to make a set of recommendations following the observations listed above in each of four areas: strategic public–private partnerships, defined legal frameworks, improvements in technological guidance, and a clear communication plan. What emerged from these individual conversations were several common themes:

- Clear Priorities are needed to effectively mobilize resources and evaluate threats to the integrity and stability of the cyber domain. There is a strong demand for comprehensive metrics designed to assess the levels of protection as they relate to a variety of potential threats to national security.
- Anticipatory Measures can help to thwart attacks and prepare for recovery in the event of disruption or denial of service. This includes the organization of response teams that are dedicated to implementing a national security policy as it relates to cybersecurity. An improvement in the current ISAC structure as well as the establishment of an early warning system for cyberattacks would enhance the integrity of U.S. networks.
- Legislative Action would enable key players to act quickly and decisively with established roles, responsibilities, and adequate funding. A critical component is a comprehensive declaratory policy from the federal government on its cybersecurity capabilities and response plans. Congressional action on regulations involving safety measures and corporate "Good Samaritan" laws as well as third party certifications of products and software were encouraged by each breakout session.
- Technical Capability is needed to develop and implement tools and procedures to limit the spread of malicious activity. Proven strategies of containment in cybersecurity would benefit private companies, especially Internet Service Providers (ISPs).
- *Education Efforts* ensure that current Internet users as well as future generations act responsibly to protect themselves and others from attack while fostering innovation in and appreciation for technological advancement. By acknowledging that every citizen is a potential target for cyberattack, the U.S. government and private industry can promote better "Internet hygiene" through improved learning opportunities. Moreover, resources should be allocated to develop and train an American cyber force dedicated to protecting U.S. networks.

Specific Conversations[1]

Strategic View: Government and Industry Partnership for National-Scale Cyberattack

The members of the Government and Industry Partnership group were charged with considering the roles of the public and private sectors in the short, medium, and long term after the events described in the "Cyber ShockWave" simulation. Specifically, they were asked to consider the fact that a majority of the computing, networking, and energy infrastructure is owned and operated by the private sector. These corporate stakeholders rarely consider investments to address rare but catastrophic events that may impact their business practices. However, these corporations will be essential in preventing and responding to national scale events. Central issues that the members were asked to consider were:

- What are the respective roles of government and industry?
- How is the transition from industry response to a government response decided?
- In order for the country to be better prepared, what concrete activities should be happening now, within three years, and within five years?

The group engaged in spirited conversation, addressing these questions. After some discussion, the panel decided to modify the questions from those originally posed, deciding to divorce the questions from the specifics of the "Cyber ShockWave" event to be more generally applicable. Hence, instead of focusing on what should be done in the one-, three-, and five-year time frames after the event, the group chose to describe instead the roles of the public and private sectors in four time frames:

- **Time Frame 1: Preparation for a possible large-scale event.** What should the public and private sectors be doing in the long term in preparation for a possible cyberattack?
- **Time Frame 2: Real time during event.** What are the roles of the public and private sector during the actual event?
- **Time Frame 3: Attribution and Response.** In the immediate aftermath of an event, what should the public and private sectors do to identify the perpetrators of the attack, and, importantly, what roles are to be played in any U.S. response (cyber, military, economic, etc.)?
- **Time Frame 4: Recovery.** In both the immediate triage and long-term recovery from an attack, how do public and private sector actors divide responsibility for repair and reconstruction?

Described below are the conclusions of the group on the roles to be played by industry and government in these situations.

[1] While none of the participants' comments are attributed, these groups were comprised of individuals from U.S. government/military, national laboratories, industry, and academia. Each participant expressed his or her individual views and not the views of affiliated organizations. In addition, each breakout session took on a unique character, which is evident in the respective tone of the summaries below.

RECOMMENDED ACTIONS (STRATEGIC VIEW):

- The government should act to create a comprehensive, real-time (24/7) system for monitoring the state of networks and control systems for the nation's most critical assets. Industry must provide accurate, timely information to this center.
- The government should assemble a commission of industry and government experts to devise a criteria-based graded-level ` threshold' standard for critical infrastructure.
- The government should take positive steps to dramatically increase the number of experts educated in cybersecurity.
- Congress should enact legislation clearly establishing the authority of the President to intercede and quarantine or shut down portions of the infrastructures to preserve the functionality of the remaining portions of those systems.
- Congress should enact a "Corporate Good Samaritan Law" shielding corporations from lawsuits and FOIA requests resulting from actions they take in a declared national cyber emergency.
- The government of the Unites States should formulate a declarative policy regarding how it views cyber attacks launched by nation states, and reserving the right to respond in whatever fashion it deems necessary to protect its interests.
- The government should have a plan for reconstruction after widespread destruction caused by a cyber attack, including clearly established responsibilities of the agencies involved.

TIME FRAME 1: PREPARATION IN ADVANCE OF ANY ATTACK OR IMMINENT THREAT

The "Cyber ShockWave" simulation demonstrated clearly that the nation lacks a sophisticated situational awareness about the states of its critical infrastructures: computer networks, Internet, financial system computer networks, cell phone systems, power grid, water systems, etc. To be sure, some of the networks (e.g., the power grid operators) do possess their own situational awareness capabilities, but they are fragmented, limited to individual provider networks, and not integrated into a coherent package. In the event of a massive, multisystem attack, accurate assessment of the state of the assets in real time will likely prove to be critical. It was also clear to all that while the industrial representatives can (and must) maintain such awareness for their own assets, no industry or even consortium of industrial partners can be expected to bear the costs or the responsibility of providing a central end-to-end awareness capability. This must fall to the government.

RECOMMENDATION: The government should act to create a comprehensive, real-time (24/7) system for monitoring the state of the computer networks and control systems for the nation's most critical assets. This capability (the group dubbed it "Computer Emergency Response Team on steroids") should provide collection and analysis of data regarding the state of the systems. This implies a responsibility on the part of industry as well. Industrial operators must be willing to provide accurate and timely information to the proposed entity regarding the state of their systems. Industry leaders observe that there is often great stigma attached to a company that admits its systems are vulnerable, let alone compromised, and that historically companies have been reluctant to share such information. This stigma must be overcome; past history of reporting outages and other kinds of reporting might provide useful insights—about both benefits and about implementation problems and other burdens.

Another aspect of the "Cyber ShockWave" simulation was clear: the participants were uncertain when the situation had grown serious enough to trigger government action. In the air travel industry, the government has established a graded threat warning system, in which threat levels are established based on criteria established a priori. There should be a similar system in place to protect the national cyber and network assets. However, given the difficulty in recognizing the immediate scope of an attack, there ought to be a graded attack-level system accompanied by a list of actions that are automatically triggered in response to a given attack level. It is important that these threat and attack levels be criteria-based, and that the responses be preplanned and practiced.

RECOMMENDATION: The government should assemble a commission of industry and government experts to devise a criteria-based graded-level 'threshold' standard for critical infrastructure. The thresholds must be clearly defined, as must the criteria that determine in which grade level a threat or actual attack resides. The commission should also create prescriptive initial responses to be employed whenever the threat/attack level passes certain thresholds.

A very real threat to American cybersecurity is the growing shortage of highly qualified scientists and engineers to conduct the fundamental research necessary to establish a credible national capability in cyber defense. The United States requires thousands of new scientists in these fields, but is only producing a few dozen of such candidates each year. Education is a crucial need for the establishment of a credible cyber defense capability.

RECOMMENDATION: The government should take positive steps to dramatically increase the number of students enrolled in programs that provide cybersecurity education. This can be in the form of individual student grants, guaranteed loans, and student loans that are forgiven if the student actually becomes a cybersecurity professional. It should also include incentives for educational institutions to create cyber programs by funding pilot programs, providing funds to create "centers" emphasizing cyber education, and funding on-the-job training and retraining efforts. While several dozen programs are in existence today, expansion of such resources would only stand to benefit the U.S. defense networks.

TIME FRAME 2: REAL-TIME ACTIONS DURING ATTACK

It was apparent to the group that rapid response was required in real time to respond to a burgeoning crisis; to whatever extent possible, the infrastructure and assets of the country must be preserved as best as possible in the face of an ongoing attack that threatens the entire system with failure or collapse. Like the participants of the "Cyber ShockWave" simulation, the group was initially divided over whether the President had the requisite authority to step in and order, for example, the quarantine and/or shut down of portions of the Internet, power grid, telecommunications network, etc., to preserve the functionality of the remaining portions of the system. In some instances the authority is clear: the Telecommunications Act, for example, provides authority to the President. The appropriate authorities are not so evident for other systems, such as computing networks or the U.S. portion of the Internet. After some discussion, there was consensus that the President must be empowered to act in defense of the systems under attack.

RECOMMENDATION: Congress should enact legislation clearly establishing the authority of the President to intercede and quarantine or shut down portions of the power grid, communications systems, computational networks, etc., to preserve the functionality of the

remaining portions of those systems. The legislation must clearly spell out the circumstances under which the President can act, the limitations to this power, and set conditions under which control of the systems must be returned to the owners and operators.

Several members of the group who represent industry suggested that, in an emergency, the owners/operators of the assets will act unilaterally to protect their systems, and that they have historically worked together to handle moderate-scale system failures in the past. Simple self-interest on the part of these businesses mandates that they act in this manner. Several group members asserted that giving the President the authority to order system shutdown or quarantine is likely to be a symbolic gesture, as the companies themselves will almost undoubtedly have already performed the actions the President would order. It should also be noted that the industrial representatives expressed great skepticism that the government possesses the technical know-how to effect a shutdown or quarantine, or even the technical expertise to recognize when such an action is an appropriate response. Despite the reluctance of industry to impose partial shutdowns or other prophylactic actions, they may be convinced that the situation is as dire as the very survival of their assets. This reluctance stems largely from two credible fears: (a) the fear that information they employ to decide their course of action or share with competitors in a mutual defense effort would be subject to FOIA (Freedom of Information Act) requests, causing the loss of industrial secrets, and (b) the fear that unilateral quarantine/shutdown actions leave them vulnerable to lawsuits for damages caused by denial of service to the portions of the systems closed off.

RECOMMENDATION: Congress should enact a "Corporate Good Samaritan Law" shielding corporations from lawsuits, and from FOIA requests, resulting from actions they may take in a declared national emergency in response to an attack on the critical infrastructures they own and operate.

TIME FRAME 3: ATTRIBUTION AND RESPONSE

In the aftermath of a major attack, there are two activities that constitute "Response" to the attack (as distinguished from "Recovery"). Specifically, insofar as is possible, there must be attribution, in which it is determined who is responsible for the attack, and then there is response, wherein the United States may choose to retaliate, punish, or take some other action against the perpetrators of the attack.

It seemed fairly clear to the group that the bulk of the actions in this time frame belong to the government. While there are roles for industry to play in attribution, it seems highly unlikely that there is any substantive role for industry in the response. Companies have neither the authority to respond, nor the legal shield against further retaliation by the bad actors. The panel felt that the attribution should be conducted under the auspices of the government, largely because the government has the authority to conduct investigations domestically, including access to the judicial system (including the FISA court, if necessary) to compel testimony, discovery and/or seizure of evidence, and to hold suspects and witnesses, all powers lacking in the private sector. If the instigators are not domestic, the government has the power of international agreement, appeal to international courts, and cooperation of international policing organizations. The role of industry in the attribution of an attack will be the free sharing of information about the attack, to provide the authorities with the necessary data to perform the attribution. For this purpose, the Corporate Good Samaritan law described earlier could be important.

It should be noted that the group was nearly unanimous in the opinion that attribution of the instigators of an attack with certainty is highly unlikely. Even identifying the machines used yields little certainty about the initiators. Attribution will always be shrouded in some degree of uncertainty, and may rely as much on traditional intelligence-gathering apparatuses as it does on technological solutions. Hence, questions of attribution and response may always be as much a political calculus as anything else. In other words, a method of ruling out potential perpetrators could help to narrow down the possible suspects in the event of a cyberattack.

It is clear that response is a government activity. The range of actions available to the government is wide. If the malefactors prove to be domestic, the legal system is available to the government. If the malefactors are international, much depends on whether they comprise a renegade organization, such as a terrorist group, organized crime, or a nation-state. If a renegade organization is responsible, the attitude of the government(s) of the country(ies) in which they reside is important.

The actions of the government in dealing with foreign-based malefactors range widely. The group noted that the government could respond with economic sanctions, a retaliatory cyber attack, or if the malefactors' attack is severe enough, even with military action. The group also noted that there currently exists no declaratory policy stating how the United States views cyber attacks brought by foreign states; absent such a policy, neither enemies nor allies have any basis upon which to form expectations as to how the United States may respond to cyberattacks.

RECOMMENDATION: The government of the Unites States should formulate a declarative policy regarding how it views cyberattacks launched by a range of actors, and reserve the right to respond in whatever fashion it deems necessary to protect its interests.

TIME FRAME 4: RECOVERY

The Recovery phase begins as soon as the attack has ended, and can last months or even years, depending on the severity of the attack. Both government and industry have roles to play in this phase. The first activity that must occur is triage, an assessment regarding the extent of the damage wreaked by the attack, and the formulation of plans to rebuild the systems that were damaged. For the most part, this assessment must be conducted by the owners/operators of the affected networks, since they possess the technical expertise to formulate the damage assessment and lay out a plan for the recovery.

The recovery and reconstruction itself also depends mostly on the industrial owners/operators, largely for the same reasons. However, in the wake of an external attack, it seems unreasonable (and likely impractical) to expect these companies to bear the costs of the reconstruction alone. If the government will need to allocate a great deal of funding to be used in the reconstruction, there will need to be means for overseeing the allocation of these funds.

RECOMMENDATION: The government should have a reconstruction plan after widespread destruction caused by a cyberattack; furthermore, the government should clarify in advance which agencies have the responsibility for ensuring that the funds are allocated and made available as needed.

Building the Policy and Legal Framework—Understanding Authorities and Roles

The purpose of this group was to clarify the legal standing with which government and industry has the capacity to act in the event of a cyberattack and what steps can be taken in the interim to prepare for such a crisis. Throughout the discussion, recommendations were made from policymakers, lawyers, academics, and technologists to create a comprehensive framework that took each sector's role into account. Although specific questions were posed to the group to stimulate the discussion, the group members addressed many of the current challenges plaguing policymakers and lawyers including: defining terms of cyber activity, identifying legal authorities, protecting civil liberties, accounting for political setbacks, and preparing for catastrophe. From here, the group proposed recommendations for concrete action in the short and long term that would best prepare the United States for future national security risks.

It was quickly determined that a common vocabulary was missing from the cybersecurity debate. Often times, policymakers find difficulty in identifying the different types of malicious cyber events based on predefined characteristics. Although it would be convenient to establish a universal definition of cyberwarfare, many experts believe that this quest is analogous to the United Nations General Assembly's attempt to define an act of aggression. With this in mind, the group took on the more fundamental challenge of applying a definition to "cyberattack."

RECOMMENDED ACTIONS (BUILDING POLICY AND LEGAL FRAMEWORK):

- Develop a metric that outlines what options are available to the United States depending on the nature and scale of the cyberattack a terms of uses of force. A clear declaratory policy regarding cyberattacks should reference the role of privacy interests as well as industry when responding to a cyber threat.
- Private companies and individuals can work to identify and block malicious code that is being routed by private ISPs and publicize bad IP addresses or eliminate them from the Internet.
- The government can use its intelligence resources to limit those who conduct malicious Internet activity.
- Congress should enact legislation that promotes transparency in privacy protections and powers given to US CERT. Clear laws and regulations that reinforce responsible behavior may be enough of a catalyst for positive change in this sector.
- Mandated information sharing could foster great cooperation as has been seen in the area of air traffic control through guidance from the Federal Aviation Administration.
- A Presidential Decision Directive for cybersecurity and enactment of a comprehensive framework for cyber defense policy would improve the possibility for an international convention for cybersecurity that includes input from the relevant parties and is incorporated into domestic laws throughout the global community.

Given the international legal model currently in place, the UN Charter is an ideal place to start the discussion of force and attack. The foundation of this debate stems from Article 2 Section 4 of the Charter, which reads:

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*

Despite such strong language, there is still confusion as to whether a use of force triggers Article 51 of the Charter, stating:

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defense shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*

A use of force typically invokes some sort of exploitation if it is carried out in a sovereign territory. As a result of the borderless nature of cyberspace, this concept presents a new challenge for legal experts both international and domestic. The military's use of the "Effects Continuum," which takes into account the 4 D's of an actual attack (Disrupt, Degrade, Deny, Destroy), could prove useful in developing a clear strategy for reacting to cyberattacks through legally established means.

RECOMMENDATION: To meet the demands of the emerging domain as it relates to national security, the United States government must develop a metric that outlines what options are available to it depending on the nature and scale of the cyberattack in terms of uses of force. From previous cases of cyber-related national security events in other states, a clear declaratory policy regarding cyberattacks will help to define the difference between an act of cyberwarfare and a threat to national security. This document would also include reference to the role of privacy interests and industry when responding to a cyber threat. Ultimately, regardless of the scale or specific target of the attack, the intent of such an event is to negatively impact the broader United States whether through critical infrastructure, government networks, or telecommunications services.

A variety of authorities already exist under federal laws that are applicable in the event of a cyberattack. The President, through the powers listed in Article II of the U.S. Constitution, is charged with defending the United States from foreign threats and domestic insurrections. In times of war, the President, as Commander in Chief, can legally compel private industry to abide by government orders if it is in the interest of national security and involves a foreign nexus. If a cyberattack were to occur, the President would be able to legally take over private networks to limit the spread of the attack if it met a certain critical threshold. Congress has also played a role in developing the current legal framework for cybersecurity through the Telecommunications Act of 1996, the USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and other parts of the U.S. criminal code. These statutes allow the President and other agencies to take action to prevent malevolent activity in the American cyber domain. Whether the mission is to stifle the spread of malware, track the movement of terrorists, or identify a hacker, existing laws are already in place that facilitate certain cybersecurity programs.

In addition to those powers, the U.S. Constitution, presidential findings, security agreements, and executive orders carry significant weight in federal policymaking especially in the realm of national security. Furthermore, international laws and customs as well as NATO policies and other international law enforcement agreements provide guidance for the United States when developing a legal framework from which to base its actions in protecting cyberspace.

The group discussed several metaphors from the kinetic sphere that can be applied to cyberspace, yet this type of analogizing has limits. Despite many attempts, one of the most basic challenges in the cyber domain is that of attribution. Due to the increasing number of potential IP addresses from which to launch a cyberattack, placing the blame on a specific group or individual is nearly impossible. While the intelligence community has access to a vast array of information sources, many experts believe that a government can never completely identify the individual perpetrator for an attack. Regardless of this fact, the government will likely be asked to step in when it comes to major attacks on private companies because industry simply cannot afford to invest in that amount of protective measures.

RECOMMENDATION: The Wild West mentality of the cyber domain has perpetuated for decades as a result of individuals and governments promoting information sharing while avoiding responsibility to protect vital networks. As twenty-first century innovation continues to progress, private companies and individuals can do their part to identify and block malicious code that is being routed by private ISPs. In addition, service providers can create a "cyber watch list" in which it publishes offending IP addresses or eliminates them from the Internet. The government can act more decisively in thwarting cyberattacks by utilizing its intelligence resources to penetrate gangs that conduct malicious activity through counterintelligence to break up trust in those actors. Such steps would lead to a more secure environment for information sharing and communication among the millions of benevolent Internet users.

The Fourth Amendment of the U.S. Constitution has been cited as a major area of contention among policymakers and lawyers when developing cybersecurity doctrine. As the provision states, Americans have the right:

> *To be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*

While there is no clearly defined right to privacy in the Constitution, many argue that the Fourth Amendment outlines what the Founding Fathers had in mind when it came to individual privacy. When it comes to developing a legal framework for cybersecurity, the group decided it was best to determine first what policies were necessary to protect the domain and then determine the legal means to justify such action. They pointed to the fact that one's privacy is not violated if information is provided to law enforcement and other officials voluntarily. Thus, the government is legally within its bounds to monitor its own networks and those of consenting critical infrastructures to detect threats. Although such analysis is surely beneficial to lawmakers and privacy advocates, uncertainty remains as to whether the government may shut down key nodes of concentrated Internet traffic into the United States if it is in the interest of national security.

RECOMMENDATION: From this part of the discussion, the group suggested that Congress enact legislation that promotes transparency not only in regard to privacy protections, but also in the power given to US CERT. This will demonstrate the government's intention to defend civil liberties as well as critical networks. Private industry may also be encouraged to take more protective action if they were shielded from potential legal action from individuals claiming privacy violations. Through clear laws and regulations that reinforce responsible behavior, the pressure of negative exposure to consumers may be enough of a catalyst for positive change in

this sector. Finally, mandated information sharing, vis-à-vis such tools as the interstate commerce clause of the Constitution, could foster great cooperation as has been seen in the area of air traffic control through guidance from the Federal Aviation Administration.

Many of the policy proposals that are suggested at workshops like "Reboot" often lack a clear understanding of political factors on the final product. With this mind, the group discussed the diplomatic regimes as well as the domestic challenges that are currently frustrating progress in the area of cybersecurity. Since there is no treaty regime for the cyber domain toward which to work as of 2010, the international community must collaborate on bilateral terms to develop security frameworks for defending against cyberattacks. The United States has been reluctant to join negotiations with China and Russia on the topic as it does not want to reveal its capabilities in this area. Still, work has been done to improve notification mechanisms for protective cyber measures in and elimination of bad actors or servers. Similar to its actions with respect to the Law of the Seas Convention, the U.S. currently is acting under customary law that relies on wide state practice, time, and international acceptance.

RECOMMENDATION: When it comes to developing a legal strategy for cybersecurity policy, lawmakers and negotiators will need to take politics into account. In the short term, this will involve inclusive discussions with a variety of stakeholders on the domestic level to create an effective Presidential Decision Directive for cybersecurity and enactment of a comprehensive framework. With this in place, the U.S. government can work with international partners to establish bilateral relationships that foster communication and cooperation to prevent cyberattacks and limit the possibility of cyberwarfare. The ultimate goal would be an international convention for cybersecurity that includes input from the relevant parties and is incorporated into domestic laws throughout the global community. It will be important to remember that such actions require significant amounts of time and resources as well as patience and compromise to reach the goal.

Finally, building a comprehensive defensive cybersecurity framework will require preparation and strategies for deterrence. The public and private sectors would do well to study the impact of monitoring and intelligence on thwarting potential cyberattacks protecting national assets and operations. A thorough risk assessment of critical infrastructure and information systems would provide policymakers and technologists with the knowledge they need to improve capabilities to limit American vulnerabilities. Congress is currently working on legislation that addresses such needs, but could also include language encouraging regulations, standards, and certifications that will improve security and promote innovation. With this in mind, it would be in the best interest of industry leaders to get out in front of legislation and develop a best-practices structure for anticipatory cybersecurity measures.

RECOMMENDATION: The group's participants were not so naïve to think that defensive measures would be implemented immediately. As the aforementioned section on the role of politics demonstrated, such policymaking takes time and patience. With this in mind, the group recommended that Congress draft and pass legislation, including amendments to existing statutes that promote safety and deterrence within the next two years. Beyond this point, an assertive effort should be undertaken to encourage research and development efforts to design and secure products and systems that are used in the U.S. cyber domain. International diplomacy as well as a strategic communication and education effort on the domestic front would help the United States to be proactive rather than reactive in its cybersecurity policies.

Technical Decision Support and Emergency Response—Improving Technical Guidance

The members of the Technical Decision Support and Emergency Response group were charged with considering how best to technically prepare and respond in the short, medium, and long term after the events described in the "Cyber ShockWave" exercise. Specifically, they were asked to consider what quality technical responses are needed in the face of rapidly advancing technology and innovation as well as the dynamic nature of the cyber threat. Central issues that the members were asked to consider were:

- What metrics are used and what do we measure to assess "secureness"?
- What technology or policy changes can make the nation more or less secure?
- How do we "predict" the technical, legal/policy, economic impacts of the threats and responses in normal situations as well as in emergencies?
- What concrete activities should be happening now, within three years and five years to be more prepared?
- What technology trends will improve or complicate national cyber security?

The "Cyber ShockWave" simulation demonstrated clearly that the nation lacks a technical understanding and situational awareness about the states of its critical infrastructures: computer networks, Internet, financial system computer networks, cell phone systems, power grid, water systems, etc. The group members were concerned that the level of information integration available to the players in the simulation (e.g., national maps of current information) do not currently exist and illustrates a technical gap. This group believed that this information is available at the level of individual companies (telco, ISP) but that even within a technology sector information sharing at this level is not available. If information integration occurs it does so on an *ad hoc* basis due to individual relationships and not due to any clear business practice or emergency response arrangements. Thus the level of situational awareness at the national level depicted in the "Cyber ShockWave" scenario is probably not accurate. That said the scenario accurately depicted the inability to technically provide the state of the critical infrastructure such as a quantitative assessment of damage, impacts of actions such as shutdown of cellular network, or likely time for containment and mitigation. The nation lacks a high-level, real-time system for maintaining awareness of the state of these critical systems. This group reaffirmed that in the event of a massive multisystem attack, a national view that accurately provided the state of the assets in real time will likely prove to be critical.

RECOMMENDED ACTIONS (TECHNICAL DECISION SUPPORT AND EMERGENCY RESPONSE):

- Near term:
  - Clearly specify criteria for identifying an asset as critical infrastructure and provide an impact weight to determine where on a continuum of possibilities the impact damage to this element would lie (e.g., inconvenience to people to loss of human life). In addition, it is necessary to identify critical elements of the U.S. infrastructure and assign initial impact weights.
  - The government bears the responsibility of defining the roles and responsibilities for decision-making in face of nation-scale event. A consortium of government and industry is needed to address the complex interrelationship between government and privately held infrastructure.
  - Specify in advance the type of information that could be needed in the face of national cyberattack. Prepare now to ensure that this information would be available to the decision makers with outages in the Internet and other services. Several pathways for delivering information must be considered
  - Evaluate the efficacy of the ISACs (Information Sharing and Analysis Centers) and leverage them more fully where they are working well while reenergizing them where they are not.
  - Immediately create teams of technical experts that are called upon in the event of a national cyber emergency. These teams should work together in advance of a major event to establish productive relationships. Team members provide expertise from all related technology areas giving the team both breadth and depth to address wide range of cyber security threats.
- Within two to three years:
  - An effort should be undertaken to create architecture for situational awareness that provides the means for information sharing from individuals, companies, and government sector entities. Technological solutions can be used to automate the integration of massive amount of data, provide tools for evaluating noise or anomalies, and address privacy concerns.
  - The government of the United States should formulate a declarative cyber warfare doctrine regarding how it views cyberattacks and determine decision command structure.
  - Better integrate cyber technical experts (outside of government) with government decision makers. Such roles may need to be incentivized to encourage technologist to serve in the government in lieu of often more lucrative private sector positions.
  - The government can incentivize academic institutions to create a robust, science-based discipline of cybersecurity where rigor and accredited curriculum is established. In addition, the government can provide scholarship programs to encourage students to pursue careers in cyber security.
- Within three to five years:
  - The government should have technical understanding on how to reconstitute services and a plan for reconstruction after widespread destruction caused by a cyberattack. Scenario planning, exercises and large-scale simulation would be needed to thoroughly understand various options and their impacts.

RECOMMENDATION: In advance of any major attack, preparation should be undertaken to determine what information would be needed and to whom. That is, determine in advance who are the decision makers for such an event and what technical information would be necessary for their decision. Once what is needed is determined, more "formal" arrangements can be made with the information custodians to provide it. Furthermore, the group expressed desire to continue scenario training as illustrated by the "Cyber Shockwave" event as an effective means to determine what the information needs would be in various situations and to determine how various actions and decisions would "play out."

In further considering the aftermath of the "Cyber Shockwave" event, two concerns were discussed. First, no clear definition exists of what comprises the nation's critical infrastructure. This will be essential for managing any major emergency; the U.S. command structure needs all the critical infrastructure elements available on a dashboard. Second, current decision makers have technical expertise when applied to classic kinetic threats as this has been acquired over decades, however, no similar technical domain knowledge and expertise exists within the current decision makers for cyber threats. The group noted that this expertise will take years to acquire and develop.

RECOMMENDATION: Until the time that cybersecurity domain knowledge is available at all levels of decision structure, actions should be taken to integrate cyber technical experts (outside of government) with government decision makers. Such roles may need to be incentivized to encourage technologists to serve in the government in lieu of often more lucrative private sector positions. In the near term, the group suggested creating a community of technical experts that could be called upon in service of the nation for any major national-scale cyberattack. This would form a way to bridge the gap between current cyber adversary's capabilities and the domain knowledge of decision makers. Furthermore in the mid-term time frame, the group suggested creating "virtual teams," groups of experts from all related technology areas necessary to address the cyber threat from industry and government. These teams would be created and exercised regularly so that trust and relationships would be established prior to any real emergency.

The topics of attribution and mitigation/recovery resulted in lively conversation without yielding consensus. As providing technical decision support was a primary theme of these discussions, the ability to provide accurate attribution for a cyber threat seemed essential. That is, without attribution information, decision makers would be reluctant to implement some of the actions that may be recommended to them. This impacts both the emergency and long-term responses to such an attack. However, given the understanding of the current state of technology, few in the group believed that accurate attribution would be achievable within the next several decades. The basis for this assessment about attribution comes from the fact that current technology was developed for capabilities without a prior concern for "secureness" and that the time scales for a major attack can occur over very long periods, making assigning the designation of who is responsible nearly impossible as it may be a generation of participants.

Many commented that no real progress has been made to date in the areas of research that enable attribution. This caused some in the group to conclude that more funding needs to be directed to this research while others concluded that, instead, funding should be directed towards research to address how to make decisions when attribution cannot be made within the timeframe of the needed decision. Given the difficulty with addressing attribution, the

focus of the conversation shifted to mitigation and recovery. Technologists believed that, in the event of a massive cyber attack, the focus needs to be on prevention of loss of life and one way to do that is to reestablish high priority services as quickly as possible. This approach concentrates efforts on rapid recovery to mitigate and contain damage rather than determining who caused the attack.

RECOMMENDATION: A large portion of the group agreed that funding resources should be focused on mitigation and recovery. Specific suggestions included creating a playbook (national book of scenarios) that described various events. Efforts would then be undertaken to develop specific courses of actions for these events. Critical infrastructure elements could "practice" against this playbook to evaluate the courses of action and evaluate the response as it pertains to metrics of recovery.

An overarching theme among the technical group was concern about the growing shortage of highly qualified U.S. scientists and engineers to conduct the fundamental research necessary to establish a credible national capability in cyber defense. Anecdotally, the vast majority of new computer scientists, mathematicians, physicists, and chemists seem to be foreign nationals, with many of them being sensitive-country foreign nationals. Thus, education of US citizens or otherwise "clearable" individuals is a crucial need for the establishment of a credible cyber defense capability.

RECOMMENDATION: The government should take positive steps to dramatically increase the number of students enrolled in programs that provide cybersecurity education. This can be in the form of individual student grants, guaranteed loans, and student loans that are forgiven if the student actually becomes a cybersecurity professional. It should also include inducements to educational institutions to create cyber programs by funding pilot programs, providing funds to create "centers" emphasizing cyber education, and funding on-the-job training and retraining efforts.

RECOMMENDED ACTIONS (RECOVERY AND COMMUNICATION):

- Implement a strategy today that considers a "Cyber ShockWave" attack and enacts reforms that should be established before a cybersecurity crisis occurs.
- An effective government communications plan after a cybersecurity attack would be tiered to best reach and address different segments of the population. In addition to addressing the American people in the immediate aftermath of a cyberattack, the President should also deliver a televised speech one month following the attack to include the following points:
  - Message to Individuals
    - We are back in business, and we understand what happened. If we know who did it, we're taking action.
    - We are in this together and are responsible for making sure that the effects for a similar attack will not be as great. Individuals, industry, and government are all responsible for cybersecurity.
    - We have existing tools to protect citizens' and government assets, and we're going to make sure they're working and shore them up (i.e. FDIC, insurance laws).
  - Message to Industry
    - We are reviewing our policies about communications.
    - We are incentivizing industry to respond appropriately and to make reform as painless as possible because industry has to provide the solution.
  - Message to Congress
    - We have to change how we do business and get the whole world on board while we don't disrupt business as usual.
- The government will need to cooperate with many actors, including industry, vendors and international partners, after an attack to ensure that the severity of such an attack in the future would be lessened. Proposed government and industry steps include:
  - Creation of a government-industry commission would include:
    - Concretely defined roles and responsibilities of all actors
    - Increased information sharing between government, industry, utilities, national labs, and citizens
    - Root cause analysis
    - Impact analysis
    - Independent, former public figures and members from the affected industries
  - Increased international engagement because of the international implications of cybersecurity.
- Encourage responsible behavior among the general public through the following strategies:
  - In the near term, the public and private sectors should educate people on technological risks and encourage individuals and companies to seek smart phone and Internet security software.
  - Within two to three years, both actors need to create a gold standard for personal security and continually update what that gold standard is.
  - Within three to five years, both actors should create mechanisms to create robust identity into the cyber world. That is, for certain transactions and sections of the Internet, individuals need to have a stronger identity because the anonymity of the Internet can shield bad actors. For instance, robust identity would better facilitate credit checks and online banking. This could also come in the form of a "secure" and "default" Internet.
- To achieve increased preparation for a cyberattack, government and industry need to be engaging in the following activities:
  - In the near term, industry and utilities need to lobby policymakers to regulate the communications industry via Congress and the administrative agencies.
  - Within two to three years, Congress should pass legislation requiring manufacturers to build in security software for smart phones and computers. The government should also declassify information to better inform industry, utilities, and individuals of the security threats. Service providers should also educate consumers when installing or selling communications technology.
  - Within three to five years, actors should cooperate to give high levels of protection on the smart grid, as well as to "harden" the power grid, communications, and Internet.
- A program that would address these issues would be multi-layered and not a centralized program. Such a program would consist of the following foundational aspects:
  - Openness and transparency, supported by admitting that cybersecurity is a problem and that the time to address it is now. Without a sense of urgency, the different sectors are unlikely to develop coherent, cohesive technology, policies, and programs.
  - Comprehensive user education vis-à-vis the government, utilities and communications service providers.
  - More responsible energy usage can help alert utilities to spikes in energy consumption, which can sometimes indicate an issue for the security of the grid. Moreover, utilities should shore up the technical capabilities of network and grids.

Recovery and Communication—Cleaning up the Chaos

This group was focused on cleaning up the chaos that developed in the final stages of the "Cyber ShockWave" simulation. This eroded public trust, causing the American people to be wary of using the Internet and other technology. Within the extension of the scenario, erosion of public trust had widespread economic, e-commerce, and information-exchange impacts. Additionally, the ability of the government and of industry to rapidly share information and mitigate emerging threats continued to be compromised.

The first main issue was trying to assess how much damage the scenario had caused to understand what the status of the country would be four weeks after the simulation. The group posited that civil unrest would probably occur in pockets of the population and that the first order of business was creating order. The group discussed the different time frames for different actors – the government might have a longer time frame for recovery than individuals, who would be considering personal impacts and would want the technological problems solved as quickly as possible. The members of this commission explained that people would no longer feel secure in their environments, even though infrastructure was probably functioning again. It was determined that the people who were localized to the crisis would be impacted more acutely.

RECOMMENDATION: First, people need to be educated on what happened and what they can do to promote responsible technology behavior after an attack. Second, government and industry need to make clear who has what authorities within their own systems as well as with each other. Finally, industry and government need to create technical solutions to better address weaknesses in technology. It was posited that new technology might help the situation, but a return to basics where fundamental security concerns remain. With a focus on education, industry and government can best explain proper usage of technology while avoiding enforcement of compliance.

RECOMMENDATION: To strengthen cybersecurity, consumers ought to purchase antivirus or security software for their smart phones, much like most computers require. In addition to relying on consumers to purchase the software, Congress should legislate that manufacturers build in security software. Again, the lack of security software on smart phones was likened to purchasing a security system without locking the doors of a home. Even if these security mechanisms did not completely eliminate cyber threats, such software would limit the impact of such an attack, rendering it an effective strategy.

The government will need to consider how it would explain the causes and effects of a cyberattack to the average American. The government would need to reach out to those with limited understanding of the technology underlying the attack. It is important that industry and the government understand what happened, and the average person needs to have information as well. The United States would also need to limit the spread of conspiracy theories (i.e. that the government planned a cyberattack to achieve a more nefarious goal). To reach as many people as possible, the group suggested a tiered message through the government as well as industry across various forms of communication. Utilities and service providers would play an important role in this stage because the attack most affected them, and those vendors have a vital stake in informing and educating their customers.

RECOMMENDATION: To responsibly assess the situation, explain events, and become better prepared for a cybersecurity emergency, the group proposed a congressional commission following an attack to conduct a root cause and impact analysis. This evaluation would need to include policy and technology countermeasures. In other words, those who invented the Internet can change it and control it. Still, there is a strong desire to see communications providers and government officials on the hook for weaknesses leading to the cybersecurity attack.

Some have argued that Congress would likely take the bully pulpit after such an incident despite the fact that it would be better to channel that energy into more substantive and productive work. Congress will want to bring in industry, the White House, and federal agencies to more fully understand the attack. This work needs to be co-opted into productive analysis and progress. While the goal for the commission would be substantive, participants argued that it would contain only elements of "Security Theater," because often the American people clamor for such activity following crises. Many believe that this commission should really be a highly moderated, independent forum to solve issues, not give actors a venue to air criticism.

RECOMMENDATION: To avoid a cyberattack in the future, some participants suggested an emphasis on information sharing between all related actors, including industry, utilities, and government. The national labs and SCADA vendors would also need to be brought into the information-sharing framework. This current lack of communication is indicative of undefined points of responsibility, including for individual citizens. The group proposed that the outlined responsibilities should be clearly articulated to clarify accountability in a crisis, which is rarely successful. Although this may take great determination on the part of key government and industry leaders, there is a strong need to emphasize the urgency of this problem to get the actors to address this issue now and just following an attack.

Some have come to rely on analogizing a cyberattack to two previous events. The first event was a letter to President Franklin D. Roosevelt about atomic energy from leading scientists in the field, including Albert Einstein. This letter encouraged President Roosevelt to utilize a group of highly educated, highly skilled scientists to develop a solution. The solution came from the scientists of the time, and they reached out to President Roosevelt first. The second case is the reform of space shuttle launches after the Challenger disaster. A similar reform effort from the private industry or from scientists could most effectively address cybersecurity. While the Manhattan Project was classified and the Challenger explosion was tragic, cybersecurity is personal. In the case of cyberattacks, a call to action may not occur until something catastrophic happens. The question remains as to who would lead such a group if this type of organization were created.

In terms of the smart grid component of the "Cyber ShockWave" simulation and the implications for utilities, participants suggested that we need to rethink how utilities are organized on networks and if there is a need to find ways to decentralize the organization to guard against such cyberattacks.

RECOMMENDATION: A Consumer Bill of Rights that establishes that consumers will not be abandoned if a service provider drops out or is destroyed through a cybersecurity disaster is essential for public trust. Not only would this be a way for companies to be held accountable to their customers, it would also ensure that they acted responsibly before or in the event of an attack.

The issue of anonymity on the Internet is a problem for attribution, especially in the case of cyberattacks. Thus, a more robust identity for Internet users on certain parts of the Internet, as well as continued "anonymity" on less important, less secure parts of the Internet, would aid investigative efforts.

Conclusion

The United States and the international community face a growing challenge in the realm of cybersecurity. As the Internet continues to expand and gain greater importance in daily life, policymakers and private industry will be forced to develop new methods for defending vital interests while protecting civil liberties. The primary purpose of "Reboot" was to link academia with science and industry to produce policy recommendations that reflect the rapidly evolving technology landscape and its cybersecurity implications.

Lawrence Livermore National Laboratory and Georgetown University have demonstrated a commitment to developing solutions to cybersecurity challenges. Beginning with a group discussion in the fall of 2009 to identify security issues related to the cyber domain, the conversation has continued with this workshop in the Spring of 2010 that focused attention on finding practical solutions to national security elements of cybersecurity. With a solid foundation to work from, the partners are dedicated to strengthening cyber defense systems within the United States through effective policy and technology.

To aid in these efforts, a collaborative research program has been established that will ensure sustained progress in the field of cybersecurity. The program has two initial focus areas:

The Human Side of Cyber Research: Establishing an Empirical Framework

- The primary objective of this research project is to develop a best-practices framework for cyber research, including safeguards to address privacy, policy, and legal issues. The project will assess the design, implementation, and enforcement of research standards. The research will adopt an interdisciplinary and comparative approach, relying on cooperation with policymakers and practitioners in the area of cybersecurity.

Tracking Cyber Threats: A Behavioral Model

- This project is designed to analyze cybersecurity-related foreign language media—of all types—to evaluate its reporting versus the English-language reporting that would be generally available to U.S. analysts. The study will be limited in scope in both time and sources, but will be innovative in applying behavioral studies to the spread of cyber threats.

The partners are encouraged by the strong interest taken in these research programs and plan to publish the results for the broader benefit to the academic and scientific communities.