Cyber Security Policy Round Table After Action Report

EXECUTIVE OVERVIEW

In October 2011, *The New School,* in conjunction with the *Richard Lounsbery Foundation,* convened *Cyber Security Policy Round Table* to examine the fundamental challenges facing the nation's cybersecurity infrastructure and discuss potential solutions that could serve as a foundation for a holistic cyber policy doctrine. *The New School* gathered a diverse set of the Round Table participants drawn from the key stakeholders in this debate, and asked them to help to develop a consensus regarding the next steps needed to bolster the country's cyber defenses and that would address the needs of all relevant parties.

The Round Table was chaired by former Senator and *The New School* President Emeritus J. Robert Kerrey, who drew upon his previous experiences as former *Member of the Senate Select Committee on Intelligence* and the *9/11 Commission* to provide valuable insight and attention to this discussion. The members of the Round Table included persons drawn from the areas of government (including federal agency employees, congressional staff, and the *Ranking Member of the House Permanent Select Committee on Intelligence),* private sector (including a director from a government defense contractor, and the CEO of a small-business), and academia (including the president emeritus of a nationally-recognized university). Round table members were asked to participate both as knowledgeable individuals and as representatives of their organizations, and to maintain confidentiality of their deliberations to promote open and candid discourse. The Round Table chose to be bound by the Chatham House Rule to maintain the confidentiality of all conversations, so that participants could converse frankly without fear of their words resurfacing at a later date.

The members of the Round Table are privileged to have had this opportunity to discuss this timely topic and to lend their personal and professional insights. All can agree that there is much work to be accomplished in this subject, and that teamwork and collaboration will be quintessential to achieving success in the coming years. This report assesses and makes recommendations in identifying the necessary steps that must be followed to secure the nation's cyber infrastructure.

THE PROBLEM AT HAND

The complex issues of cybersecurity and cyber warfare have emerged as critical threats facing the United States. Yet even today, as the details of such threats have become much clearer, the United States Government has failed to deliver a cohesive cyber policy doctrine that protects us from potential nightmare scenarios. Indeed, the pace at which technologies are emerging that are capable of doing the U.S. harm is far greater than the pace our policy makers have been able to advance legislation to react accordingly.

As many scholars and economists have pointed out, the Internet and other associated technological advances through the 1990s and up to today have helped to create an environment that allowed for a dramatic expansion of globalization and interconnectivity of world markets. To be sure, many benefits have come from the ability to operate quicker, leaner and more efficiently through cyberspace. However, as the world becomes more dependent on cyberspace as a conduit to improve efficiencies of all kinds, it must also be attuned to the threat that this dependence creates.

The Internet was originally conceived to be a place for the free and open exchange of ideas, academic research and other activities for positive change. It was not originally thought to be a central repository of secret information and encrypted data. Therefore, the responses to security concerns have been met with a patchwork of enhancements (cyber firewalls and other similar technologies) that do not fully address the fundamental security problems of the cyber environment.

In addition, the anonymity of cyberspace allows for individuals to compare products, assess market competition and engage in a host of other activities that a free and open society is built upon. However, this anonymity also opens the door to malicious actors being able to operate with impunity behind a cyber cloak to, for example, take a power grid offline or cause an oil pipeline to explode. The now very real threat of non-kinetic warfare by both state and non-state actors is something that could cause irrevocable harm to the United States in a very short period of time.

The cyber threats facing America are ever-expanding in the target-rich environment of the Internet. The Department of Defense (DoD) alone has 3.5 million computers and 35 internal networks in 65 countries, many of which depend on commercial systems. According to a 2001 report from the General Accountability Office (GAO), DoD identifies and records thousands of "cyber events" daily, some of which are determined to be attacks against systems and networks. On June 16th, 2011, the CIA's

PIIM PARSONS INSTITUTE FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

public website experienced distrusted denial of service (DDOS) throughout the evening, which a group of hackers calling themselves "Lulz Security" took credit for.

Of course, threats are not limited to federal systems. In fact, private sector companies are equally at risk, yet lack many of the security controls necessary to prevent unauthorized access. Just recently, Sony Corporation revealed that hackers had stolen personal and billing information for up to 100 million people, while Google revealed that it had been the subject of a major espionage attack originating in China aimed at stealing personal information about human rights activists. Fox News has also suffered several embarrassing hacks on its Twitter account, one of which falsely reported that President Obama had been shot. As recently as early June 2011, both Automatic Data Processing, Inc. (ADP) and the International Monetary Fund's (IMF) security controls were compromised. The IMF's breach was so significant that the World Bank cut the computer link that allows the two institutions to share information. On May 21st, 2011, Lockheed Martin detected and thwarted "a significant and tenacious attack on its systems.

Clearly, the issue of cybersecurity has transcended the boundary between the public and private sector and has become a crucial component of national security.

FEDERAL AUTHORITIES

Multiple agencies within the federal government have jurisdiction over cybersecurity. These entities include the Department of Defense, the Department of Homeland Security, the Department of Justice (including the Federal Bureau of Investigation), the Department of State, and the National Security Agency. Each of their duties is outlined in the following section. It should be noted, however, that because of the ambiguous nature of attacks, and inability in many cases to distinguish between an act of war and a small-scale event, many agencies have overlapping roles and responsibilities.

Department of Defense (DoD)

As part of its mission, the Department of Defense (DoD) is responsible for protecting and defending its networks, including establishing relationships with other entities to share computer vulnerability data and coordinate activities and operations. As such, DoD has the lead in protecting the ".mil" domain in the internet. As a federal department with cybersecurity expertise, DoD is required by the Homeland Security Presidential Directive 7 (HSPD-7) to coordinate with the Department of Homeland Security (DHS) to secure cyberspace.

Department of Homeland Security (DHS)

The Department of Homeland Security is responsible for preventing and deterring terrorist attacks and protecting against and responding to other threats and hazards within the United States, including key resources and critical infrastructure. Under federal law and policy, DHS has been tasked with strengthening international cyberspace security in conjunction with other federal agencies, international organizations and industry. Thus, DHS is the designated lead in protecting the ".gov" and ".com" domains in the Internet.

Department of Justice (DoJ)

The Department of Justice is the chief law enforcement agency of the US government and is responsible for prosecuting violations of cyber-related laws such as the *Computer Fraud and Abuse Act*. HSPD-7 directs DoJ to coordinate with DHS, and also with international organizations and countries to strengthen critical infrastructure and key resources of the United States. DoJ officials have also stated that the department has a role in the activities of the International Sub-IPC.

Federal Bureau of Investigation (FBI)

The FBI has a unique dual responsibility, to prevent harm to national security as the nation's domestic intelligence agency and to enforce federal laws as the nation's principal law enforcement agency. These roles are complementary, as threats to the nation's cybersecurity can emanate from nation-states, terrorist organizations, and transnational criminal enterprises; with the lines between sometimes blurred. As a member of the U.S. Intelligence Community (USIC), the FBI leads the National Cyber Investigative Joint Task Force (NCIJTF). Finally, HSPD-7 directs the FBI to work with DHS in dismantling and mitigating cyber threats.

Department of State (DoS)

As the lead U.S. agency with responsibility for foreign affairs, the Department of State has a variety of duties relating to cyberspace. It is responsible for the formulation, coordination and oversight of foreign policy related to international communications and information policy, including primary authority for determining U.S. positions and the conduct of U.S. participation in negotiations with

PIIM PARSONS INSTITUTE FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

foreign governments and international bodies. It is also responsible for the coordination and oversight with respect to all major science and technology agreements. In addition, under the 2003 *National Strategy to Secure Cyberspace,* the department is to lead federal efforts to enhance international cyberspace security cooperation. Finally, HSPD-7 requires the Department of State to coordinate with DHS on cybersecurity-related issues.

National Security Agency (NSA)
The National Security Agency (NSA) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO). The Information Assurance mission confronts the formidable challenge of preventing foreign adversaries from gaining access to sensitive or classified national security information. The Signals Intelligence mission collects, processes, and disseminates intelligence information from foreign signals for intelligence and counterintelligence purposes and to support military operations.

PENDING CYBER LEGISLATION

Across the federal government, there exist a multitude of statues that address various aspects of cybersecurity both directly and indirectly. However, Congress has yet to enact legislation that will set forth an overarching framework. While revisions to most of the statutes have been proposed over the past few years, no major cybersecurity legislation has been passed since 2002.

Recent proposals have focused largely on issues in ten areas, yet have remained somewhat broad in scope. These areas include national strategy and the role of government, reform of the *Federal Information Security Management Act (FISMA)*, protection of critical infrastructure, coordination between the public and private sector, personal information data breaches, cybercrime, electronic privacy, international efforts, research and development and the cybersecurity workforce. Several of these proposals have received committee and/or floor action, but all have failed to become law.

Proposals have been offered by both the House of Representatives and the Senate. However, each chamber's approach to enacting legislation differs in both substance and approach. The House tends to prefer to address cybersecurity in a number of smaller related bills that address all necessary aspects of cybersecurity, while the Senate has continually pursued a comprehensive bill that encompasses all issues at once. The following represents an examination of both chambers' proposals.

Cybersecurity Act of 2012 (s.2105)
The *Cybersecurity Act of 2012* directs the Secretary of Homeland Security (DHS), in consultation with owners and operators of critical infrastructure, the Critical Infrastructure Partnership Advisory Council, and other federal agencies and private sector entities, to:

> *(1) to conduct a top-level assessment of cybersecurity risks to determine which sectors face the greatest immediate risk, and beginning with the sectors identified as having the highest priority, conduct, on a sector-by-sector basis, cyber risk assessments of the critical infrastructure; (2) establish a procedure for the designation of critical infrastructure; (3) identify or develop risk-based cybersecurity performance requirements; and (4) implement cyber response and restoration plans.*

The bill also sets forth requirements for securing critical infrastructure, including notification of cyber risks and threats and reporting of significant cyber incidents affecting critical infrastructure. Additionally, it defines "critical infrastructure" as systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, or national public health or safety.

The bill amends the *Federal Information Security Management Act of 2002 (FISMA)* to revise information security requirements for federal agencies and provide for continuous monitoring of, and streamlined reporting of, cybersecurity risks and amends the *Homeland Security Act of 2002* to consolidate existing DHA resources for cybersecurity within a National Center for Cybersecurity and Communications. The duties of the Center would include managing efforts to secure, protect, and ensure the resiliency of the federal information infrastructure, supporting private sector efforts to protect such infrastructure, prioritizing efforts to address the mostsignificant risks to the information infrastructure, and ensuring privacy protections.

PIIM PARSONS INSTITUTE FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act: SECURE IT (S. 2151)

The Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, & Technology (SECURE IT) Act would update the current federal IT security law, the Federal Information Security Management Act (FISMA), while maintaining the roles of the National Institute of Standards and Technology (NIST) and the Department of Commerce in overseeing security standard for the federal government.

In addition, SECURE IT would also require federal telecom and IT security contractors to report to the government cybersecurity threats related to their services, while strengthening criminal statutes for cybersecurity crimes or violations. The bill emphasizes the importance of research and development, as well as partnership between the private and public sectors in the creation of expedited information sharing system, and de-emphasizes federal regulation. Instead, the act relies on a series of government incentives to ensure that companies comply with protecting critical infrastructure in the private sector.

Recommendations of the House Republican Task Force

House Speaker John Boehner and Majority Leader Eric Cantor formally created the Cybersecurity Task Force in June and charged the group with making recommendations in four key areas: authorities, information sharing and public-private partnerships, critical infrastructure, and domestic legal frameworks. While the final report was not an actual legislative proposal, the recommendations would instead be used to influence future bills in Congress.

The recommendations emphasize need for the improvement of existing information sharing structures and the development of an active defense capability, as these efforts would improve security and disseminate real-time information to help counter cyber adversaries. Additionally, the report suggests the use of voluntary incentives to encourage private companies to improve cybersecurity, such as the development of voluntary standards through a public-private partnership, utilizing existing tax credits and grant funding to promote increased security, and studying the possible role the insurance industry may play in strengthening cybersecurity.

Another section of the report discusses the need to update several federal laws that pertain to cybersecurity. These include the Federal Information Security Management Act (FISMA) of 2002, Computer Fraud and Abuse Act (CFAA) of 1986, as well as other communications laws and criminal statutes. Finally, the report states that updating legal authorities is among the most complex issues facing lawmakers. It recommends certain areas where Congress should begin, including defining a proactive process for Defense Support of Civil Authorities (DSCA) and increased support from the Department of Defense to the broader federal government. The report also suggests that Congress should formalize the Department of Homeland Security's current role in coordinating cybersecurity for federal civilian agencies' computer and networks.

OBSERVATIONS

To understand the context of the recommendations being set forth in this document, the Round Table operated under the assumption of the following five observations. Through a discussion of each of these topics, the Round Table was able to make policy recommendations regarding the nation's cybersecurity infrastructure.

1. The United States has an exponentially increasing dependency on computer networks and information infrastructure.

Cyberspace and the flow of information are involved in virtually every aspect of the nation to some degree, including commerce, education, national defense, recreation, and the federal government's operations. The nation's growing dependence on its information infrastructure was highlighted by a 2011 report by the General Accountability Office, which concluded that dependence on information systems to carry out essential everyday operations makes it vulnerable to an array of cyber-based risks. Simply put, it is this dependence on cyber systems for support of national activities that creates new vulnerabilities that can be exploited by both domestic and foreign state and non-state adversaries. As government, private sector, and personal activities continue to move to networked operations, the threat will continue to grow.

2. The country faces a wide range of cyber threats from both state and non-state adversaries.

Threats to interconnected computer systems are continually evolving and increasing in complexity and scope. The major threats identified include those posed by criminal groups, foreign intelligence services, hackers, insider threats, and information warfare from both state and non-state actors.

PIIM PARSONS INSTITUTE FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

These groups and individuals have a variety of attack techniques at their disposal that can be used to determine vulnerabilities and gain entry into targeted systems. For example, phishing involves the creation and use of fake e-mails and Web sites to deceive Internet users into disclosing their personal data and other sensitive information.

The connectivity between information systems, the Internet, and other infrastructures also creates opportunities for attackers to disrupt telecommunications, electrical power, and other critical services. Even private sector companies, especially those linked to the public sector, face the threat of cyber-attacks. Significant among these is the March 2011 attack against RSA, in which their SecurID security tokens used by many federal agencies were compromised. The attack forced RSA's parent company to replace all 40 million tokens in circulation at that time, costing the company over $66 million.

Despite these instances of cyber-attacks, the community of national security analysts is now only beginning to grapple with the implications of the new threats and what they mean for cyber warfare with adversaries.

3. There is a growing gap between the demand for qualified cyber professionals and current workforce levels.
Given the nation's dependence on cybersecurity and the resulting interconnectedness between industries, effective cybersecurity is critical to the sustainability and safety of the nation. As a result, the federal government must ensure that a highly trained and qualified cyber workforce exists to actively serve as the first line of defense. However, there is currently a large disconnect between the demand for cyber professionals and existing candidates. According to the "Cyber IN-security: Strengthening the Federal Cybersecurity Workforce" conducted by Booz Allen Hamilton in 2009, 33% of cybersecurity management professionals, including chief information officers (CIOs) and hiring managers, were unhappy with candidate quality.

4. The constantly evolving nature of cyber threats outpaces the federal government's ability to respond and negates their efforts to adequately protect the nation.
Cyber attackers have grown increasingly sophisticated. The impact of this evolution is seen not only in the scope and nature of cyber security incidents, but also in the range of actors and targets. In the last year, the nation observed increased breadth and sophistication of computer network operations by both state and non-state actors. Despite technical advancements in detection and attribution that shed light on malicious activity, cyber attackers continue to explore new means to circumvent defensive measures. As noted by James Clapper in his February 2012 testimony to the House Permanent Select Committee on Intelligence, the nation currently faces a cyber environment where emerging technologies are developed and implemented faster than governments can keep pace, as illustrated by the failed efforts at censoring social media during the 2011 Arab Spring revolutions in Tunisia, Egypt, and Libya.

5. A large portion of critical infrastructure is owned by the private sectors, who share a responsibility with the federal government to protect civilian networks.
85% of the nation's critical infrastructure is owned or operated by the private sector. Pervasive and sustained computer-based attacks pose a potentially devastating impact to systems and operations and the critical infrastructures they support. Because the private sector owns most of the nation's critical infrastructure, such as banking, telecommunications and electric grids, it is vital that the public and private sectors form effective partnerships to successfully protect these cyber-reliant critical assets from a multitude of threats including terrorists, criminals, and hostile nations.

RECOMMENDATIONS

Based on the observations listed above and the discussion that were held during the Round Table, the following recommendations have been set forth.

1. Streamline the federal hiring process to allow for the inclusion of more "white-hat" hackers in federal agencies.
The federal government has a notoriously cumbersome hiring process, which deters talent of from entering government service, and there are many other system problems that raise challenges for the cybersecurity workforce. A repeated concern is that there will be a shortage of qualified cyber professionals in the coming years to help protect the nation's cybersecurity infrastructure. Congress should reform the way cybersecurity personnel are recruited, hired, and trained to ensure the federal government has the talent necessary to lead the national cybersecurity effort and protect its own networks. Such talent could be drawn from the pool of

PIIM PARSONS INSTITUTE
FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

non-traditional ethical hackers, or "white-hat" hackers.

However, many of these individuals lack the requisite security clearances (as a result of ineligibility) while others view employment by the federal government as a negative. These types of "white-hat" hackers could provide a major benefit to the federal government, as they are more adept at predicting behaviors of malicious actors, understand underground hacking tools and tactics, analyze net traffic and thus identify vulnerabilities in federal systems. As the traditional recruiting efforts of the military and government agencies have not effectively paired with the hacker community, the federal government risks losing valuable assets in the hacker population to illicit/improper activity that exacerbates the problem of internet policing, data theft, and loss of intellectual property.

The federal hiring process must be reformed to allow for an increase in the number of non-traditional, ethical hackers in the federal cybersecurity workforce. This would allow for the creation of a new type of workforce that would elicit support from these individuals to lend their skills and talents to the federal government without the need for security clearances. Once the federal government has identified those individuals who fit the necessary profile, it could hire and provide them with the training they would require to operate successfully in a DoD or DHS environment.

2. Establish a "white-hat" training program for civilians to voluntarily police the Internet in their spare time to identify and remove malicious code from infected computers of the general populace.
The Department of Defense is currently struggling with the question of how to "Man, Train and Equip" a competent cyber workforce capable of not only defending DoD, and potentially non-DoD networks, but when directed, execute full-spectrum computer network operations against our adversaries. The "Cyber Battlespace" is an ever-changing, incredibly dynamic environment that a finite number of elite communities have actually already begun to master and are potentially several years ahead of the DoD in terms of capability and capacity. However, these unique individuals lack the leadership, guidance and discipline to be a true cyber workforce capable of focusing their efforts towards U.S. objectives.

The federal government must engage non-federal partners and create a public-private partnership to develop a "cyber-badging program through an academic institution and then identify the "white-hat" types of individuals and provide them with the training they would require to operate successfully in a DoD or DHS environment. This would allow for the federal government to create a workforce of a civic-minded, academically approved community of ethical hackers.

The Department of Defense has already begun to explore the idea of a reserve civilian cyber workforce, identified by their willingness to serve and the capabilities they immediately bring to the table. The problem has been to identify those individuals and groups who not only have know-how but that have also been conditioned to work under the direction of senior government officials and potentially uniformed officers directing their efforts. The badges earned by the individuals identified and trained in a program would give these civilians the same level of credibility as their military and government counterparts, but would already possess the technical knowledge needed to be able to contribute to the mission faster than a newly identified recruit that requires many years of both technical and military training before they can be operational.

3. Raise public awareness and perception of the need for comprehensive cybersecurity.
As previously stated, the nation has grown increasingly dependent on online activities to manage all aspects of daily life, yet remains mostly unaware of the cyber dangers that threaten the privacy, safety and financial security not only of themselves but also the broader nation. Americans must be made more aware of the tools and practices that can help protect them from the negative consequences that cyber threats represent. A variety of outlets exist that should be employed to communicate, including thorough awareness campaigns, public service announcements, technical conferences, business roundtables, media channels, and competitive grant solicitations to develop "best practices" for dissemination.

The federal government, in conjunction with private sector partners, must develop standards and strategies for digital literacy training for the American population to ensure that the public can use tools and techniques to reduce risk in the cyber environment. Federal entities with jurisdiction over cyber issues should actively engage educators to raise awareness among students about the dangers of and mitigation tools available for cyber activity. Through these tools, the public awareness of cyber threats can be drastically increased to improve the overall safety of the nation's cyber infrastructure.

PIIM PARSONS INSTITUTE FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

4. Establish science, technology, engineering and math (STEM) education and workforce pipelines that begin at the secondary-school level with the end goal being to bolster the cyber workforce of the nation.
The academic pipeline begins with STEM, particularly math, in elementary and secondary school. Cultivating this interest early on leads students to pursue careers in the areas of science and mathematics through high school and college. However, on average the nation's high school students are well behind those students of foreign states in mathematics and science testing. Additionally, most high schools do not offer rigorous computer science courses that focus on computational thinking. Instead, these courses are often focused on the use of standard office products and enhancing typing skills. As a result, most computer science students enter college with a subpar grasp of computer science and little understanding of both the intellectual aspects of cybersecurity and the potential careers in the subject. Not surprisingly, there has been a steady decline of students choosing to pursue information technology careers.

The nation can produce the next generation of the cybersecurity workforce by bolstering student interest in STEM and cybersecurity subjects beginning in elementary school and maintain that interest through challenging and unique courses throughout their education. Courses must teach students to be creators of technology, rather than users, and raise awareness of the potential of a career in cybersecurity. Additionally, the federal government must not only create partnerships with entities capable of providing instructional materials for K-12 cybersecurity and STEM education and but also align computer science curriculum across the nation to focus on the promotion of computer science and cybersecurity as a career, rather than simply for user functions. Quintessential to this will be the participation of non-federal actors. The education system must leverage the role of teachers, parents and private business to improve STEM education to better prepare and support students in following this endeavor.

5. Explore novel technologies, including those that contain decentralized systems with multi-layer verification processes and auditable, role-based access capabilities.
The security community faces a challenging paradox with today's cybersecurity methodologies: the need for a high level of security but also the need for easy access to secure data. This paradox renders inadequate the centralized security model based on firewalls and simple logons.

Under current data access methodologies, authorized users enter their credentials into established web-based portals for verification. Some approaches, such as those used by RSA, go a step further by using two-factor authentication such as tokens with number codes that rotate on a timer. However, there are two problems associated with this process: permanent web-based portals are stationary targets for hackers to attempt to bypass attheir leisure, and no process exists to determine if a user's credentials have been comprised (and are being used by the user himself or an unauthorized individual). As a result, novel technologies must be explored that can alleviate the problems with currently accepted cybersecurity access methods.

Such technologies should include non-traditional methods for accessing data, including but not limited to:

- Elimination of the need for public servers while still providing secure access to sensitive data via the Internet;
- Strong dual-factor authentication through the use of a token to validate user credentials to launch the application;
- Use of a virtual software application that exists only in RAM and only when the session is active;
- An automatic "flush" of all data and cookies from RAM when the session is terminated; and
- Multi-layer security and role-based access

Profound benefits can be gained through the implementation of a technology with a combination of the aforementioned capabilities. By developing a virtual software application that erases itself clean when a user terminates their session, the military and private companies could not only have improved auditable, secure transfer of data, but also the potential to eradicate the threat of residual data in-theater. For instance, this technology could be used in the case of a downed drone behind enemy lines to erase all software from the hardware of the drone. The federal government should explore and implement pilot programs that test innovative solutions that could help strengthen the nation's cyber infrastructure.

PIIM PARSONS INSTITUTE FOR INFORMATION MAPPING

Website Address:
http://piim.newschool.edu/cyber

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

6. Streamline federal agencies' roles and responsibilities in the cyber arena to promote better coordination and to aid in the defense of the private sector.
While internet security is a responsibility requiring the coordination and cooperation of many different actors, the current federal oversight is too thinly dispersed among the federal agencies. As a result, a pattern of bureaucracy and confusion exists among law enforcement and government agencies working to combat cybercrime. Federal entities tasked with a role in cybersecurity include the Department of Defense (DOD), the National Security Agency (NSA), the Department of State, the Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI). DOD contains the United States Cyber Command is responsible for attacks on its networks, while the NSA is at least nominally part of DOD. The State Department concerns itself with diplomatic security, the FBI with law enforcement, and DHS with counterterrorism. The agencies are supposed to coordinate their effort through the president's cybersecurity coordinator Howard Schmidt, the "cybersecurity czar" who was named to the post in 2009.

While in theory, each agency is responsible for a different aspect of cybersecurity, the reality remains somewhat murkier. Agency are competing to become the dominant entity for cybersecurity issues within the federal government, and simultaneously attempts to amass more responsibility while refusing to cede its current authority to another. As a result, the current federal cybersecurity landscape is at best, confusing and bureaucratic. The federal government must understand that there is only one Internet, and thus the only vector for hostile actors to initiate cyber-attacks. Agencies must streamline and coordinate their efforts to better protect against cyber-attacks through the sharing of information and cooperation on complex threats.

Similarly, this coordination must also apply to the private sector. Cyber threats against the private sector are no different than those against federal networks. While the scale, scope, and purpose of the attack may differ, the method remains the same and requires the same types of preventative technology, planning, coordination and information sharing. The federal government has dedicated a substantial amount of funding to cybersecurity initiatives, and subsequently learned a great deal from those programs that could help private industry make their systems and data more secure. However, if there are no clear mechanisms in place to help conduct knowledge transfer between public and private industry, these programs are greatly wasted on being solely in the province of the federal government. Efforts have been made to accomplish this, such as the Defense Industrial Base (DIB) pilot, but more is needed to fully achieve this goal.

7. Define critical infrastructure of the civilian economy not covered under CYBERCOM, including the electric power grid, water supplies and the financial system, and harden their cyber defenses.
Threats to systems supporting critical infrastructure are evolving and growing. In February 2011, the Director of National Intelligence testified that, in the past year, there had been a dramatic increase in malicious cyber activity targeting U.S. computers and networks. As defined in the House Republicans' "Recommendations of the House Republican Cybersecurity Task Force," critical infrastructures are specific physical assets, functions, and systems that facilitate the production and distribution of goods and services that are necessary for a functioning nation, such as power distribution, water supply, and telecommunications. The nation's increasing dependence on computerized industrial control systems to monitor and control equipment that supports modern critical infrastructures renders these functions increasingly susceptible to code that alters these control systems to inflict serious damage.

The government should work closely with each sector to identify the portions of critical infrastructure that, if damaged or destroyed, could cause great loss of life or significant economic damage impacting national security and work to establish a plan to monitor and protect these previously identified elements. However, there are differing opinions on the ways in which to promote cooperation between the federal government and the private sector.

Some believe that the best way to ensure compliance is to require it through federal legislation. This approach has been adopted by the Cybersecurity Act of 2012. DHS would be required to conduct sector-specific evaluations and implement cybersecurity plans to prevent against catastrophic attacks. However, opponents claim that this approach is too intrusive and could result in unforeseen costs to the nation. Other options, such as those outlined in the SECURE IT Act and the *Recommendations of the House Republican Cybersecurity Task Force,* instead advocate for voluntary incentives for companies to

PIIM PARSONS INSTITUTE
FOR INFORMATION MAPPING

68 5th Avenue
Room 200
New York, NY 10011

T: 212 229 6825
F: 212 414 4031
http://piim.newschool.edu

ensure compliance and protection, and consider regulation to be "government overreach." However, one point is clear: the critical need to come up with some kind of plan has been emphasized by officials such as FBI Director Robert Mueller, who has said that he expects the cyber threat to surpass the threat of terrorism in the near future.

CONCLUSIONS

Cyberspace has permeated almost every facet of modern society and provides critical support for the U.S. economy, civil infrastructure, public safety, and national security. However, while there are many benefits to the ease of access to the Internet, its openness has also aided in the rise of malicious actors. Unfortunately, the nation is still not equipped to handle the rise in threats from state and non-state adversaries who seek to exploit the weaknesses of the nation's dependence on its cyber infrastructure to cause harm. As President Obama said in 2009, "It's now clear this cyber threat is one of the most serious economic and national security challenges we face as a nation." While the federal government has undertaken progress in remedying identified deficiencies, there is still much work that must be done before the nation's cyber infrastructure can be comfortably secure. Without future action, many of today's problems will only increase in the not-too-distant future.

Currently, the government is not optimally organized to address the issue of cyber security in an effective and efficient fashion. As stated, current pipelines are ineffective and federal hiring practices are antiquated and inefficient. As a result, many of the nation's talented individuals with the most potential to help secure the nation's networks are being overlooked or driven away. Education and hiring practices must be reformed to allow for the nurturing and hiring of individuals who can contribute to the nation's cybersecurity posture.

Additionally, responsibilities for cybersecurity are scattered across a numerous federal departments and agencies, many with overlapping authorities, and who are attempting to position themselves as the supreme federal entity in charge of the issue. The government needs to coordinate among these agencies so as to promote an effective network that can protect the nation against cyber adversaries.

Research on novel technologies to help protect the cyber infrastructure is inadequate. The government needs to increase investment in research that will help address cybersecurity vulnerabilities while remaining cost-effective and efficient. Furthermore, much of the critical infrastructure that the nation depends on today is owned by the private sector. As such, an effective solution to strengthen and protect these entities requires a public-private partnership. The government must also evaluate the strongest method to creating this partnership—whether it is through a regulatory approach or through voluntary incentives.

Ultimately, the United States must act now to mitigate the vulnerabilities in its cyber infrastructure that result from its growing reliance on cyberspace. This will require leadership and cooperation between the entities that comprise the federal government, engage the private sector more effectively and develop new strategies, policies and capabilities. While the issue of cybersecurity is a responsibility of every person, the federal government should lead the effort and help to engage the rest of the nation in the discussion and effect positive change to securing the national cyber infrastructure.