SECURING CYBERSPACE THROUGH PUBLIC-PRIVATE PARTNERSHIP

A COMPARATIVE ANALYSIS OF PARTNERSHIP MODELS

Rachel Nyswander Thomas

May 2012

(Updated August 2013)

Table of Contents

EXECUTIVE SUMMARY

Though the term "cybersecurity" has only recently penetrated the American psyche, concern among policymakers about the need to better secure cyberspace has been intensifying for nearly two decades. The threat of cybercrime and state-sponsored attacks is growing, and cyber threats are evolving rapidly.[12] Today, cybersecurity is a national priority, and public-private partnership (PPP) is understood as a vital tool in securing cyberspace.

Despite the proliferation of cybersecurity PPPs over the past decade, the literature suggests that such efforts have often suffered from ill-defined goals and objectives, a lack of clearly articulated strategy, and a focus on information sharing as a goal rather than a tool. In light of such criticism, this paper asks, and seeks to answer, a foundational question: what model of PPP is most appropriate for the task of securing cyberspace? Four PPP alternatives are proposed and analyzed, from which one alternative is identified for implementation. A strategy for implementation is recommended for the chosen alternative.

[1] Lord, K. & Sharp, T. "America's Cyber Future: Security and Prosperity in the Information Age." Center for a New American Security. (2011, June). Vol. 1 & 2.
[2] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).

ACKNOWLEDGMENTS

In the course of my research, I have been overwhelmed by the generosity of experts willing to speak with me about the challenges of bringing public and private entities together in fruitful partnership. Their enthusiasm for my inquiry speaks to the need to forge a better path for public-private partnership in cybersecurity.

In particular, I would like to acknowledge the contributions made to this project through a series of interviews conducted with more than a dozen individuals. The background information – as well as anecdotal insights – each provided were invaluable in shaping the analysis and recommendations made here. These individuals requested that they not be named; they are cited throughout the paper simply as "personal communication."

I would also like to thank Professor Matthew Fleming, for his invaluable guidance in honing my understanding of complex policy problems, and fine-tuning the resulting analysis and recommendations.

Finally, I would like to thank Professor Steve Smith for opening my eyes to the discipline of public-private partnership, and giving me the tools necessary for the endeavor of improving the way we work with one another on pressing policy challenges.

INTRODUCTION

"A technology that can give you everything you want is a technology that can take away everything that you have." – *Daniel Geer, Chief Information Security Officer, In-Q-Tel*

The dangers of cyberspace are increasingly familiar to the American public. Cyber attacks may target the online banking credentials of a small U.S. business, the networks of the largest and best-resourced multi-national corporation, or the email passwords of prominent U.S. officials.[3] The perpetrators of these attacks are domestic citizens, overseas terrorists or criminals, and even foreign governments. The victims are equally diverse: private citizens experiencing identify theft, businesses losing intellectual property, federal agencies suffering breaches of confidential information, and shareholders affected by falling stock prices.

The damage caused by cyber attacks is not limited to the virtual realm – it can include physical destruction and even human fatalities[4] – but the most common harm is to the U.S. economy.[5] A 2011 Ponemon Institute study of fifty companies across a range of industries found that such businesses suffered an average of $5.9 million in costs related to cyber crime per year. Some organizations experienced losses as high as $36.5 million per year, with smaller organizations suffering a significantly higher per capita cost than their larger counterparts.[6] The theft of technology, research, and intellectual property through cyber crime are harder to quantify, but are similarly detrimental to the economy as a whole, weakening U.S. investments in

[3]

[4] Lord, K. & Sharp, T. "America's Cyber Future: Security and Prosperity in the Information Age." Center for a New American Security. (2011, June). Vol. 1 & 2.

[5] "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2008, December.) http://Csis.org/media/pubs081208_securingcyberspace_44.pdf.

[6] Ponemon Institute. Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies. (August 2011) http://www.ponemon.org/library/2011-second-annual-cost-of-cyber-crime-study-benchmark-study-of-u-s-companies

innovation while boosting the research and development capacities of perpetrators.[7] Such damage has a throttling effect on the economic power of the Internet, which has enabled the U.S. annual gross domestic product (GDP) to grow by an estimated $2 trillion and contributes approximately $6,500 per capita to GDP every year.[8]

According to the Obama Administration's 2009 Cyberspace Policy Review, the threat of cybercrime and state-sponsored attacks is growing.[9] The threats themselves are evolving rapidly as well.[10] Today, Congress and federal agencies are targeted with an estimated 1.8 billion cyber attacks per month.[11] In 2011, the U.S. Computer Emergency Readiness Team (US-CERT) estimated that attacks against the Internet and networks of federal agencies alone increased almost 40 percent over the previous year .[121314]

Today, cybersecurity is a national priority, and public-private partnership (PPP) is considered to be a vital tool in securing cyberspace.[1516] The past decade has seen the creation of many PPPs seeking to answer the call for greater cybersecurity. However, the literature suggests

[7] Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2011, January). Washington, DC.
[8] Lord, K. & Sharp, T. "America's Cyber Future: Security and Prosperity in the Information Age." Center for a New American Security. (2011, June). Vol. 1 & 2.
[9] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).
[10] Ibid.
[11] Ibid.
12 Statistics such as these are often criticized as lacking strong evidence or concise meaning. They are included here simply for context, and to provide a sense of scale.
13 Statistics such as these are often criticized as lacking strong evidence or concise meaning. They are included here simply for context, and to provide a sense of scale.
[14] "Monthly Activity Summary," U.S. Computer Emergency Readiness Team, September 2011, http://www.us-cert.gov/press_room/monthlysummary201109.pdf.
[15] The Cyberspace Policy Review states that "the public and private sectors' interests are intertwined with a shared responsibility for ensuring a secure, reliable infrastructure upon which businesses and government services depend." Additionally, it states that "only through such partnerships will the United States be able to enhance cybersecurity and reap the full benefits of the digital revolution" (White House, 2009). Approximately 80-90 percent of all critical infrastructure is privately owned and operated (Government Accountability Office [GAO], 2010b). Further, the private sector holds considerable expertise in the development of Internet policy, creation of cyber technology, and defense against network intrusions (CNAS, 2011).
[16] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).

that many of these efforts have suffered from ill-defined goals and objectives, a lack of clearly articulated strategy, and a focus on information sharing as a goal rather than a tool.[17] The Government Accountability Office (GAO) reports that the U.S. has not yet succeeded in creating a type of partnership that would adequately account for the divergent expectations and incentives of public and private entities.[18] The Center for Strategic and International Studies (CSIS) has gone so far as to say that PPP is a failed remedy that should be set aside in favor of new concepts and strategies.[19] In light of such criticism, this paper asks a foundational question: what model of PPP is most appropriate for the task of securing cyberspace?

That PPPs have yielded limited success to date is unsurprising given the shifting sands upon which such partnership efforts have been built. Experts have yet to agree upon what it means to secure cyberspace – in particular, whether the primary goal of cybersecurity efforts should be protection, deterrence or resilience. The concept of a cybersecurity PPP is no less murky: while many partnerships continue to focus singularly on information sharing, the literature suggests the need for collaboration across a host of objectives, including research and development, building human capital,[20] technical standard setting to ensure interoperability, and the development of domestic and international policy.[2122]

---

[17] Lewis, James A. "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2008, December.) http://Csis.org/media/pubs081208_securingcyberspace_44.pdf.

[18] Government Accountability Office. Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed. (GAO Publication No. GAO-10-628). (Washington, DC: GPO, July 2010)

[19] Lewis, James A.,"Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2011, January). http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

[20] Lewis, James A., "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters" Center for International & Strategic Studies. (2010, November.) http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf

[21] Lord, K. & Sharp, T. "America's Cyber Future: Security and Prosperity in the Information Age." Center for a New American Security. (2011, June). Vol. 1 & 2.

[22] White House, Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program, (Washingon, DC: U.S. Government Printing Office 2011).

This paper begins with a review of the history and authorities that inform the use of PPP as a tool to secure cyberspace. Next, a survey of the current landscape of cybersecurity PPPs is undertaken to determine whether any change from the "status quo" is necessary to achieve the nation's cybersecurity goals. The following chapter seeks to reframe the current concept of cybersecurity PPP, informed by the application of partnership theory to this particular policy area, and to determine the requirements for an ideal cybersecurity PPP. In this context, the next chapter proposes and analyzes four PPP alternatives in order to identify the most appropriate alternative for implementation. The final chapter outlines a recommended strategy for the implementation of the best alternative before concluding thoughts are presented.

RELATED HISTORY AND AUTHORITIES

This chapter reviews the history and legal authorities informing the use of PPPs to secure cyberspace, as it is important to understand the historical and legal environment in which any cybersecurity PPP must operate.

PARTNERSHIP TO SECURE CRITICAL INFRASTRUCTURE

The federal government has a long history of involvement in the regulation of privately held technological infrastructure, beginning with Congress authorizing President Woodrow Wilson to assume control of telegraph systems during World War II.[23] The creation of the Federal Communications Commission (FCC) in 1934 and the Department of Commerce's National Institute of Standards and Technology (NIST) in 1965 moved the federal government toward a model of setting parameters within which the private sector could develop and manage information technology. [24]

It was not until three decades later that a modern concept of a PPP to protect information technology and other critical infrastructure began to develop. With Presidential Decision Directive 63 (PDD-63) of 1998, President William J. Clinton established the protection of critical infrastructure and key resources (CIKR) as a national goal and called for cooperation between the government and the private sector to protect physical and cyber-based systems.[25] A structure was established under White House leadership to coordinate efforts within the federal government and the private sector, to "eliminate any significant vulnerability to both physical

[23] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).
[24] Ibid.
[25] White House, Presidential Decision Directive 63: Policy on Critical Infrastructure Protection, (Washington, DC: U.S, Government Printing Office, 1998).

and cyber attacks on our critical infrastructures, including especially our cyber systems."[26] To foster public-private coordination, PDD-63 encouraged the development of Information Sharing and Analysis Centers (ISACs) that could be tasked with gathering, analysis, and disseminating of information to facilitate the protection of CIKR. Despite the directive, only a handful of the CIKR sectors – including financial services, communications and supply chain management – had created ISACs by the time the U.S. suffered the attacks of September 11, 2001 (9/11).

POST-9/11 ERA PARTNERSHIP

Shortly after 9/11, Congress passed the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, specifically addressing the need for sharing of information between the public and private sectors in order to secure critical infrastructure (2001).

In 2002, the Homeland Security Act created the Department of Homeland Security (DHS) and mandated the implementation of procedures for federal agencies to share both classified and unclassified information with state and local entities, as well as the private sector.[27] That same year, the Critical Infrastructure Information Act reorganized many of the existing efforts related to the CIKR protection and placed them under DHS. Of these existing structures, the National Cyber Security Division (NCSD) became the lead department responsible for working with public, private, and international entities to secure cyberspace and the United States' cyber assets.[28]

[26] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).
[27] Homeland Security Act of 2002, Pub. L. No. 107-296, §116, Stat. 2135 (2002).
[28] Government Accountability Office. Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience. (GAO Publication No. GAO-10-296). (Washington, DC: GPO, March, 2010)

This consolidation and restructuring of cybersecurity efforts continued in 2003 when the Bush Administration launched the first National Strategy to Secure Cyberspace.[29] The 2003 strategy supplemented and partially superseded PDD-63, establishing a policy by which federal departments and agencies could identify and prioritize CIKR with the aim of protecting it from terrorist attacks. [30]

The ISAC infrastructure continued to develop during this period. By 2003, ten of the eighteen CIKR sectors had established ISACs. Given that neither PDD-63 nor HSPD-7 called for regulatory enforcement of the public-private coordination, the growth of the ISACs was due solely to voluntary participation by the private sector in both information sharing and policy advising activities.

In 2004, Congress mandated additional reforms to enhance information sharing within the federal government, and with the private sector. The Intelligence Reform and Terrorism Prevention Act established the Office of the Director of National Intelligence (ODNI) to coordinate intelligence and information sharing among federal agencies, and directed the Bush Administration to create an Information Sharing Environment (ISE) through which information regarding terrorist threats could be shared with the private sector.[31]

The establishment of a National Infrastructure Protection Plan (NIPP) in 2006 provided another avenue for PPP. In addition to requiring that each CIKR sector create a Sector Specific Plan (SSP), the NIPP called for the establishment of the Critical Infrastructure Partnership Advisory Council (CIPAC), which created Sector Coordinating Council (SCC) structures

[29] White House, The National Strategy to Secure Cyberspace, (Washington DC, US Government Printing Office, 2003).
[30] Ibid.
[31] Berkeley, A. R. III, Bush, W., Heasley, P. G., Nicholson, J. B., Reid, J. A., Wallace, M. J. Intelligence Information Sharing: Final Report and Recommendations. National Infrastructure Advisory Council. January 10, 2012 http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

through which the private sector could facilitate related information sharing and policy development.[32] Similar Government Coordinating Council (GCC) structures were created to coordinate government agencies in a similar manner. The Information Technology (IT) Sector Specific Plan (IT SSP) contains DHS's framework for a coordinated national approach to cyber threats and vulnerabilities that pose risks to the nation's IT critical infrastructure.[33]

FROM CRITICAL INFRASTRUCTURE TO CYBERSECURITY

The Bush Administration introduced a Comprehensive National Cybersecurity Initiative (CNCI) in 2007.[3435] The CNCI was intended to bridge the gaps between law enforcement, intelligence, counterintelligence, and military efforts to address the full spectrum of cyber threats from remote network intrusions and insider operations to supply chain vulnerabilities. It declared DHS as the agency responsible for coordinating federal efforts to secure cyber infrastructure across all industry sectors, in conjunction with designated sector-specific Executive Branch agencies.[36] The CNCI also defined the term "cyberspace" as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries," providing focus for related efforts by the public and private sectors. [37]

Building on the CNCI, President Barack H. Obama announced a 60-day cyber policy review during his first year in office. The resulting Cyberspace Policy Review, released in May 2009, reinforced the vital nature of partnership between the private sector and government in

[32] Ibid.
[33] Congressional Research Service. Critical Infrastructures: Background, Policy and Implementation (Washington, DC: GPO, 2011)
[34] The Comprehensive National Cybersecurity Initiative (CNCI) was formalized as National Security Presidential Directive (NSPD) 54 / HSPD-23.
[35] Ibid.
[36] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).
[37] Ibid.

order to effectively secure cyberspace.[38] The review called for improvements in cybersecurity across all CIKR sectors. To accomplish this, it recommended an evaluation of barriers that continued to impede the evolution of cybersecurity PPP. Additionally, it called for greater partnership in developing a framework for incident response, enhanced information sharing to improve such incident response capabilities, encouragement of innovation in the field of cyber technology, and improved partnership with the international community.

In the wake of the Cybersecurity Policy Review, President Obama reinforced the importance of cybersecurity by declaring cyberspace a critical national asset that the United States would use all means to defend on May 29, 2009.[39] This declaration put pressure on federal agencies to find ways to work successfully with one another – as well as the private sector – and they acted quickly to adjust their policies and practices accordingly. For example, the Department of Defense (DOD) announced the creation of a Cyber Command in June 2009, signed a memorandum of understanding (MOU) with DHS to foster collaboration on cybersecurity and other issues in September 2010, and released a DOD Strategy for Operating in Cyberspace in July 2011. DOD's cyber strategy notes specifically that clarifications in policy and operational roles will make it easier for agencies to partner with one another in a manner that increases mission effectiveness and conserves limited budgetary resources, ultimately improving its ability to work with DHS in public-private partnerships.[40]

Presidential Policy Directive 8 (PPD-8) on National Preparedness, released in March 2011, recognized the necessity of PPP in the context of "strengthening the security and resilience

[38] Ibid.

[39] Lewis, James A.,"Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2011, January). http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

[40] Department of Defense. Department of Defense Strategy for Operating in Cyberspace. (Washington, DC: GPO, July 2011)

of the United States through systematic preparation for the threats that pose the greatest risk to the security of the Nation" – including cyber attacks.[41] PPD-8 specifically calls out the private and nonprofit sectors – as well as individual citizens – as bearing responsibility for national preparedness along with all levels of government, and calls for coordination between public and private actors toward that end.[42][43]

The need to strengthen such partnerships was reinforced further in the National Security Strategy released by the White House in May 2010. The strategy notes that PPPs – domestic and international – must address a host of issues including laws regarding cybercrime; the development of norms of conduct in cyberspace; standards for data preservation, protection and privacy; as well as network defense, intrusion investigation and unified response to cyber attacks.[44]

As the White House and federal agencies have strengthened their focus and strategy relating to cybersecurity, the private sector has also undergone organizational changes making it better suited to participation in cybersecurity PPPs. Executive positions designed to increase security and facilitate government interaction are now common throughout the business community. Increasingly, corporate Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) assume the additional duty of representing their organizations in the appropriate PPPs aimed at securing cyberspace.

[41] White House, Presidential Policy Directive 8 on National Preparedness, (Washington, DC: U.S. Government Printing Office).
[42] Ibid.
[43] Ibid.
[44] White House, National Security Strategy, (Washington, DC: U.S. Government Printing Office, 2010).

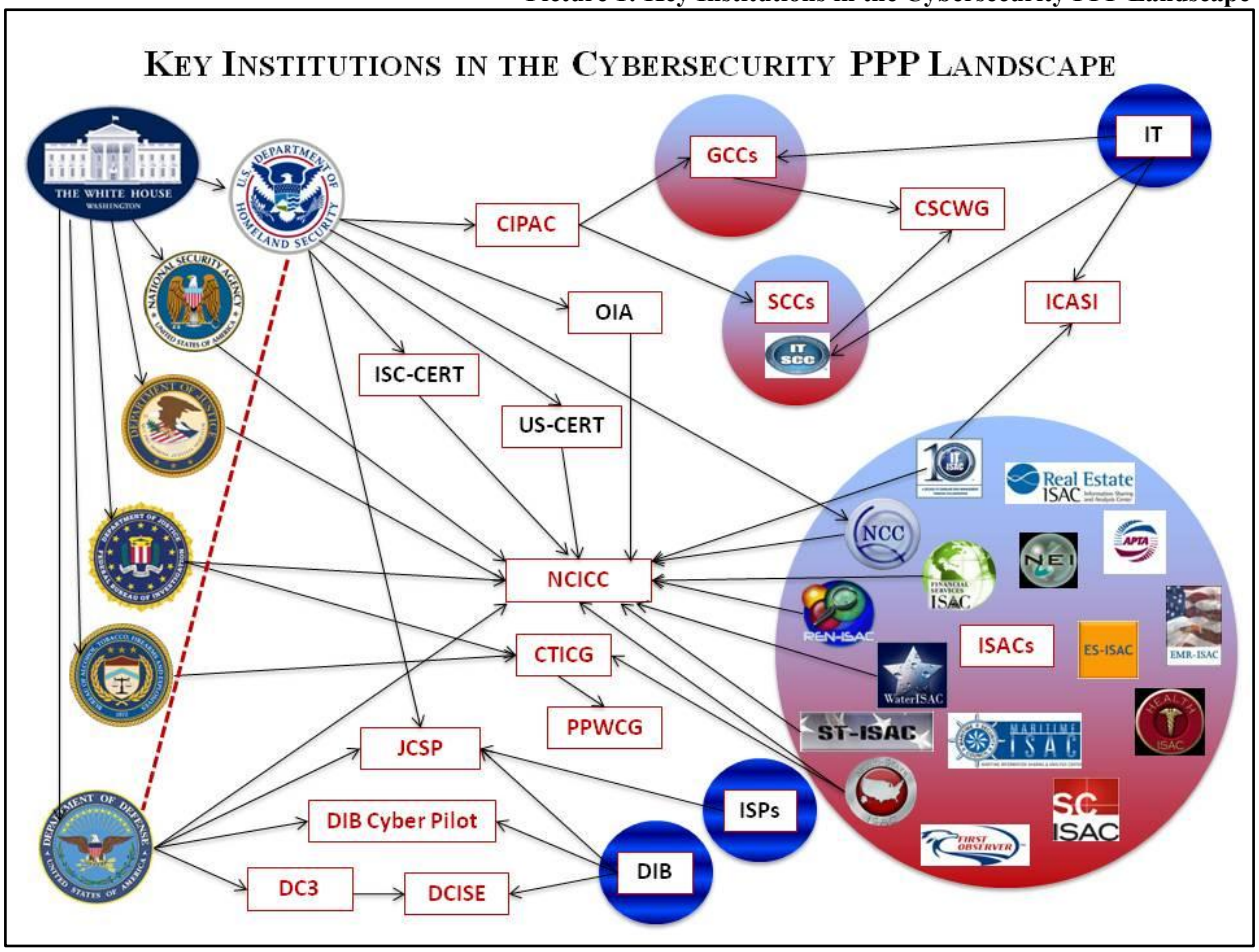
CYBERSECURITY PARTNERSHIP TODAY

This chapter analyzes the landscape of PPPs currently working to secure cyberspace in order to assess the usefulness of PPP as a cybersecurity tool. It examines several representative examples of cybersecurity PPP before providing a critical analysis of the status quo.

THE CURRENT LANDSCAPE

There are a host of PPPs aimed at securing cyberspace in existence today, as well a considerable universe of private-private and public-public partnerships (see Picture 1).

Picture 1: Key Institutions in the Cybersecurity PPP Landscape



Sources: Numerous, including ISAC Council; Center for Internet Security; Department of Defense Cyber Crime Center; DHS website; DHS Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot; and White House Cyberspace Policy Review.

By and large, these partnerships focus on information sharing – sometimes defined as the sharing of cyber threat information – though some address other objectives relating to cybersecurity, such as the development of cyber policy or the coordination of response to cyber incidents.

INFORMATION SHARING AND ANALYSIS CENTERS

There are sixteen Information Sharing and Analysis Centers (ISACs) operating today.[45] PPD-8 envisions ISACs as facilitating the protection of CIKR from a full-range of both physical and virtual threats.[46] While their early history focused on physical threats, many ISACs have increased their focus on cybersecurity as the infrastructure that controls and manages CIKR moves increasingly to virtual platforms, creating complex interdependencies between physical and cyber threats.

Each ISAC focuses on sharing information about cyber threats related to its own industry. Today, most operate as non-profit organizations, including several that started under government auspices.[47] Many have membership structures that engage organizations operating within that sector. For example, membership in the Financial Services ISAC (FS-ISAC) includes financial services providers, security firms, government agencies, law enforcement bodies and other trusted sources of information related to the security of the banking and finance industry.[48] The Multi-State ISAC (MS-ISAC), which works to improve the cybersecurity of state, local,

[45] National Council of ISACS. "About Us." (2012) http://www.isaccouncil.org/.
[46] White House, *Presidential Directive 63: Policy on Critical Infrastructure Protection*, (Washington, DC: US Government Printing Office).
[47] Anonymous, personal communication, 2012
[48] Financial Services Information Sharing and Analysis Center. "About the FS-ISAC." (2012) http://www.fsisac.com/about/.

territorial and tribal governments,[49] convenes senior technical and management executives from every state and more than 200 local governments, including all fifty state capitals, many large counties and large urban areas.[50]

Created as focal points for gathering, analysis and dissemination of information, ISACs provide their sectors with services that facilitate the sharing of information regarding cyber threats, threat alerts, risk mitigation and incident response. The information sharing that occurs through ISACs may be in the form of briefings and white papers, threat calls and webinars, or anonymous reporting. Several of the most mature ISACs have 24-hour security operations centers through which cyber threat information constantly flows from affected entities to others at risk within the sector.[51] These formal centers grew largely out of informal sharing arrangements, some of which were able to form initial sharing relationships and build trust among competitor members without formal disclosure agreements in the post-9/11 environment.[52] Such sharing has since evolved into highly formalized operations centers, some with their own "traffic light protocols" to guide the types of information that can be shared with various partners.[53]

While the ISAC network has matured greatly over the past decade, the levels of industry engagement and coordination vary significantly from sector to sector.[54] Perhaps unsurprisingly, sectors with a long history of federal regulation and private-agency collaboration, such as banking and finance, were the first to organize and develop protection strategies. Key ISAC

[49] Multi-State Information Sharing & Analysis Center, "Multi-State Information Sharing & Analysis Center: Mission & Objectives." Accessed August 15, 2013. http://msisac.cisecurity.org/about/.
[50] Anonymous, personal communication, 2012
[51] Anonymous, personal communication, 2012
[52] Ibid
[53] Ibid
[54] Government Accountability Office. (2006, October). Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics. (GAO Publication No. GAO-07-30). (Washington, DC: GPO, October 2006)

leaders cite long-standing and trusted working relationships as key to the success of the most developed ISACs.[55] In contrast, several CIKR sectors have yet to organize ISACs. Though ISAC leaders note that the volume and quality of information shared within and across ISACs has improved significantly in recent years, it remains unclear whether this trajectory of increased sharing will lead to a fully developed – and inter-connected – ISAC environment, or if gaps in the information sharing environment will remain.[56]

GOVERNMENT COORDINATING COUNCILS & SECTOR COORDINATING COUNCILS

Whereas ISACs focus on the sharing of information, Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) are intended to focus on the development of policy to enhance the protection of each CIKR sector, including cyber assets.

Within the IT sector, the IT GCC and IT SCC are the federally-mandated forums for developing and communicating public and private perspectives and developing collaborative policies, strategies, and security efforts to advance infrastructure protection – including a specific focus on cybersecurity policy.[57] The IT GCC is comprised of representatives from federal, state and local governments with responsibilities for cybersecurity. The IT SCC includes a broad base of owners, operators, associations, and other entities within the IT sector who come together to consider and publish policy positions, integrate the development of such policy with other sectors, and review existing policy over time.[58] IT-SCC coordinates among its private sector parties and works with the IT-GCC to develop IT sector recommendations for cybersecurity preparedness, response and recovery best practices.[59]

---

[55] Ibid.
[56] Anonymous, personal communication, 2012
[57] Congressional Research Service. Critical Infrastructures: Background, Policy and Implementation (Washington, DC: GPO, 2011)
[58] Information Technology Sector Coordinating Council. "Overview of the IT-SCC." (2012) http://www.it-scc.org/.
[59] Ibid.

The IT GCC and IT SCC coordinate through the CIPAC.[60] While CIPAC's mandate is the protection of CIKR in every sector, its Cross-Sector Cyber Security Working Group (CSCSWG) enhances the development of cyber-related policy within and among the SCC and GCCs in each of the CIKR sectors, bringing together the ISAC Council, US-CERT, and other ad hoc groups as needed.[61]

While the SCC and GCC structures were designed as policy-making counterparts to the ISACs, they do participate in information sharing regarding cyber threats – such as common vulnerabilities – as well as sharing information about best practices and policy positions.[6263]

NATIONAL CYBERSECURITY AND COMMUNICATIONS INTEGRATION CENTER

Operating under the DHS Office of Cybersecurity and Communications (CS&C), the National Cybersecurity and Communications Integration Center (NCCIC) is a 24-hour center for the sharing of cyber threat information across government entities – federal, state and local government, as well as the intelligence and law enforcement communities – and the private sector.[64] While direct sharing between the ISACs is still somewhat inconsistent, several of the individual ISACs now share information simultaneously with one another and government entities through the NCCIC.[65]

---

[60] Congressional Research Service. Critical Infrastructures: Background, Policy and Implementation (Washington, DC: GPO, 2011)
[61] Copeland, G.,"National Infrastructure Protection Plan (NIPP) Partnership Model and Cross Sector Cyber Security Working Group (CSCSWG)." 2010, April 27 http://www.dtic.mil/ndia/2010DIBCIP/TuesdayCopeland.pdf.
[62] This overlap between the ISAC environment and the SCCs and GCCs speaks to the complicated interplay of PPP models currently in existence.
[63] Information Technology Sector Coordinating Council. "Overview of the IT-SCC." (2012) http://www.it-scc.org/.
[64] Department of Homeland Security. About the National Cybersecurity and Communications Integration Center (NCCIC). August 9 2011 http://www.dhs.gov/xabout/structure/gc_1306334251555.shtm.
[65] Anonymous, personal communication, 2012

NCCIC serves as the national response center during a cyber or communications incident.[66] Its six functional branches focus on facilitating the sharing of information between NCCIC and its public and private partners; enriching knowledge of existing and emerging threats through examination of data shared between its partners; developing recommendations to mitigate emerging threats; coordinating incident response efforts among its partners; developing strategic plans to respond to and manage real-world emergencies; and coordinating deployment of DHS personnel to incident sites in order to analyze, contain and mitigate the effects of cyber emergencies.[67]

On the secure NCCIC floor, cyber threat information flows in from the DOD, Department of Justice (DOJ), Federal Bureau of Investigation (FBI), U.S. Secret Service and the National Security Agency (NSA), as well as DHS elements including US-CERT, the Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), the National Coordinating Center for Telecommunications (NCC), and the DHS Office of Intelligence & Analysis.[68] The representatives of these federal partners are joined on the NCCIC floor by representatives of ISACs that have been given the necessary security clearance to participate in NCCIC activities. To date, at least five ISACs have representatives on the NCCIC floor and several more are expected to join the list soon.[69]

The full-time coordination of government agencies and industry sectors on the secure NCCIC floor has made it possible to partially overcome one of the biggest barriers to effective information sharing: the intelligence classification system. Rather than needing to decouple cyber threat information from details about the related actors, declassify the appropriate

[66] Ibid.
[67] Ibid
[68] While the NCC is part of DHS, it was designated as the ISAC for the telecommunications industry in 2000 (NCC, 2011). This is another excellent illustration of existing organization infrastructure being refocused on PPP for the purposes of cybersecurity.
[69] Anonymous, personal communication, 2012

information and disseminate it throughout the private sector, private sector representatives are given security clearance to join government partners in a secure environment where they can view classified information, coordinate directly in understanding and fighting existing threats, and partner in mitigating future threats. In this way, public partners build trust in the private sector by literally inviting their private sector counterparts inside government constructs. They benefit from the sector-specific knowledge that their private partners bring to the NCCIC environment, which fosters the trust of government actors in their private sector counterparts. In this way, NCCIC allows for the creation and sharing of common knowledge across both sectors, while also providing a physical environment that fosters trust relationships on both sides of the public-private equation.

The NCCIC model is a promising one, but significant barriers remain in moving information out of the secure NCCIC environment and into the broader private sector in order to effectively fight and deter cyber threats. The declassification issue reemerges when cleared partners look to carry threat information off the NCCIC floor to warn those in the rest of the private sector about the particular threats of which they should be aware. For example, only 200 people in the entire financial services sector have a clearance level that would enable them to receive classified information directly from ISAC partners on the NCCIC floor.[70] Thus, the enhanced ability to identify and fight threats built in the NCCIC environment is difficult to extend to others in the private sector – or even government entities without clearances – except in the form of very general best practices not related to specific incidents or threats. Thus, private sector partners on the NCCIC floor must be expert not only in cybersecurity technology, but also in translating classified threat information into general, but still actionable insights for those operating in an unclassified world.

[70] Anonymous, personal communication, 2012

Questions also remain about whether NCCIC will prove an effective nexus for cybersecurity information sharing, threat mitigation and strategic planning across all of the CIKR sectors. Without a fully mature ISAC in every sector, NCCIC lacks a qualified partner in several key areas of the private sector. Further, the effectiveness of NCCIC's efforts – whether its activities around sharing, mitigation and planning have resulted in a reduction in cyber threats, or even more effective management of those that exist – have not yet been formally studied.[71]

A HOST OF FOCUSED EFFORTS

In addition to the formal partnerships for public-private information sharing and policy development codified in the ISACs, SCCs, GCCs, and NCCIC, a host of smaller and more focused partnerships are working to secure cyberspace. While an exhaustive examination of these smaller partnerships is not possible here, it is worth examining a few representative efforts.

While ISACs, SCCs and GCCs connect public and private partners in a particular sector, there is a set of related partnerships that focus solely on connecting private sector actors within one sector with one another. One such example is the Industry Consortium for Advancement of Security on the Internet (ICASI), a private-to-private partnership focused on cybersecurity information sharing and policy development in the IT sector. ICASI was founded in 2008 by eight of the largest IT companies – all but one of which also helped to found the IT-SCC.[72] ICASI's mission is to create a "forum of trust" in which industry leaders can work together to address security challenges and mitigate operational risks, as well as drive innovation in Internet security and develop industry best practices.[73] ICASI developed a Unified Security Incident Response Plan (USIRP) that enables its members to "analyze and mitigate international and

[71] James A. Lewis, in personal communication with author, February 2012.
[72] While ICASI's mission is similar to that of the IT-SCC, its membership is limited to only the largest IT industry stakeholders, while IT-SCC encompasses a set of actors more diverse in size and function.
[73] Industry Consortium for Advancement of Security on the Internet. "About Us." (2012) http://www.icasi.org/.

multi-vendor IT security challenges" and is working to create a Common Vulnerability Reporting Framework (CVRF) that would enable disparate actors to assimilate their security-related data sets via a standard format.[74] While both the USIRP and CVRF are undoubtedly necessary tools in the global effort to secure cyberspace, the fact that they are being developed without broader industry engagement – or formal participation from public sector entities – may limit the likelihood of their adoption as global standards.

In addition to national partnerships, a series of regional organizations are focused on cybersecurity information sharing. For example, the Cyber Threat Intelligence Coordinating Group (CTICG) brings together multi-state actors to work on both physical and cyber protection for critical infrastructure specifically in New York State.[75] The CTICG was created in the aftermath of the 9/11 attacks out of recognition that trust was key to facilitating the type of information sharing that would prevent future attacks, whether physical or virtual. CTICG brings federal agencies – including the FBI, DHS, Secret Service and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) – together with state and local government agencies and law enforcement to share threat information and partner in related investigations. A subgroup within the CTICG, the Public-Private Cybersecurity Working Group, has begun regular meetings that include New York State regulators and leaders from the businesses they regulate in the financial services, energy and utilities sectors.[76] While many of the actors involved in the CTICG are the same as those in the MS-ISAC, the type of information sharing is different: MS-ISAC has a secure environment in which to share highly sensitive threat information, whereas CTICG meetings are intended to share unclassified information with only an informal "for your eyes

[74] Ibid.
[75] Anonymous, personal communication, 2012
[76] Anonymous, personal communication, 2012

only" designation, extending the sharing from MS-ISAC to a level where it can be translated into tactical response at the regional and local levels.[77][78]

While most PPPs work to secure private sector cyber infrastructure regardless of the data traversing private networks, a subset of partnerships are not only sector-specific, but also focused on the security of a particular subset of online information. For example, within the Defense Industrial Base (DIB), several partnerships focus solely on securing federal and military information that is stored and transferred over private sector systems. The DIB Collaborative Information Sharing Environment (DCISE) is one such clearing house aimed at protecting DOD content traveling over and residing on corporate networks (Department of Defense Cyber Crime Center [DC3], 2012). Launched in 2008, the DCISE provides an information sharing forum for DOD and dozens of DIB companies, as well as a collaborative environment in which threat information products are designed to increase cybersecurity across the DIB. The DCISE model provides two important incentives for private sector engagement: access to a suite of cybersecurity products available only to participating companies, and anonymization of private sector intrusion reports before the information is passed to DOD.[79] These incentives are vital in an industry where public and private partners have starkly different cybersecurity concerns: government approaches cybersecurity information sharing as a public good and a national security necessity, while industry players may harbor serious concerns that information shared about intrusions will reduce their competitive advantage in bidding for future government contracts. While decades of close public-private engagement have given the DIB stakeholders familiarity with one another, the added incentives of product access and anonymized reporting

[77] The CTICG example of extending trusted relationships through information sharing partnership at the local level is a promising one, but rather unique. Other regions and localities may find it difficult to replicate the type of intense interest that made the creation of CTICG possible more than a decade removed from the 9/11 attacks and in geographic areas less intimately tied to those events.
[78] Anonymous, personal communication, 2012
[79] Anonymous, personal communication, 2012

have enabled DCISE participants to build strong trust relationships over the past five years of partnership.[80]

Recent pilot projects have built upon both the NCCIC and DCISE concepts to strengthen public-private cybersecurity partnership specifically in the DIB sector. In 2010, DOD launched a six-month DIB Cyber Pilot in which the government shared classified threat intelligence with a handful of private DIB companies, enabling the private partners to strengthen their own network defenses and provide added protection to the DOD content in their possession at an incremental increase in cost.[81] By providing intelligence directly to the private sector, concerns about government access to private sector networks were avoided. Industry partners reportedly stopped hundreds of intrusions during the pilot. Given this initial success, DOD and DHS announced in January 2012 that they are undertaking a "proof of concept" in the form of a Joint Cybersecurity Services Pilot (JCSP) involving both DIB companies and their Internet service providers (ISPs).[82] The stated purpose of the JCSP is identical to that of the DIB Cyber pilot, but DHS will manage the information sharing relationship with the ISPs in this new iteration.[83] While still focused on the DIB sector for now, the JCSP gives new energy to the concept of handing government intelligence to the private sector such that private entities can better secure their own systems without actual government intervention.

One potent criticism hangs over this seeming leap forward in effective cybersecurity PPP: it is not clear that the information shared by DOD in the DIB Cyber Pilot was responsible for the hundreds of intrusions stopped by private sector partners. One source notes that only two of 52 malicious activity incidents detected over the course of six months were found using government

[80] Ibid
[81] Lynn, W. J. III. (2011). "The Pentagon's Cyberstrategy, One Year Later: Defending Against the Next Cyberattack." Foreign Affairs: Volume 90 (issue 5).
[82] Department of Homeland Security. Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot (JCSP). (DHS/NPPD-021.) (Washington, DC: GPO, January 13 2012)
[83] Ibid.

information, as opposed to information obtained by the DIB companies through independent investigation of their own networks.[84] These reports raise questions about the extent to which public-private information sharing is necessary to improve cybersecurity, if the intelligence shared by the public sector is little better than the information already in the hands of private partners.[85]

CRITICAL ANALYSIS OF THE STATUS QUO

This survey of existing PPP models highlights several successes and challenges facing public and private actors seeking to partner in securing cyberspace. Existing cybersecurity PPPs can be credited with creating a strong infrastructure for information sharing and – to a lesser extent – policy development, as well as with increasing coordination within and across each sector. Further, this PPP infrastructure is generally not designed with a focus on a particular type of cyber threat, ensuring that PPPs can continue to provide value as threats and related technologies evolve. This is particularly vital in an area as quickly evolving as Internet technology, where advances in cloud computing, mobile devices, artificial intelligence and broadband expansion will undoubtedly lead to new cyber threats at every turn.[86]

To date, PPPs have successfully built trust in small pockets and reduced barriers to cross-sector sharing. This has been possible, in part, because intra-governmental coordination has also improved significantly, fostered by advancements such as President Obama's declaration of

[84] Corrin, A. (2012, January 18). "DOD gives DHS expanded role in cybersecurity program." Defense Systems. http://defensesystems.com/articles/2012/01/18/dib-cyber-pilot-dhs-dod.aspx.
[85] If the JCSP produces similar results, it may lend credence to the importance of private actors sharing with one another through forums like ICASI, and highlight a role for government in facilitating private-to-private sharing rather than acting as an information sharing partner itself.
[86] Lord, K. & Sharp, T. "America's Cyber Future: Security and Prosperity in the Information Age." Center for a New American Security. (2011, June). Vol. 1 & 2.

cyberspace as a critical national asset; the development of a memorandum of understanding (MOU) between DHS and DOD; and the creation of Cyber Command within DOD.[87]

Significantly, these PPP successes have been accomplished without congressional action to encourage partnership. Rather, both public and private actors have recognized the vital need to better secure cyberspace and acted voluntarily toward that end. While legislative mandates require various agencies to protect the federal government's generic Top Level Domain (gTLDs) – DHS for .gov and DOD for .mil – there is no equivalent mandate for private sector gTLDs such as .com, .info or .net. Rather, their defense from every cyber attack to date has been through the voluntary efforts of the private entities that manage them, with aid from public counterparts. Given the failure of the 112th Congress to pass comprehensive cybersecurity legislation, and continued gridlock on the subject in Washington, DC, this willingness to partner voluntarily may continue as the primary force driving the advancement of PPP to secure cyberspace in the near future.

These voluntary PPP efforts have also met significant challenges along the way, many of which continue to hinder progress toward the goal of securing cyberspace. For example, the lack of agreement about the appropriate definition for "critical cyber infrastructure" has made it difficult to identify and engage all of the key stakeholders necessary to secure such critical assets. To date, experts continue to disagree as to whether cybersecurity PPP must extend across all eighteen CIKR sectors in order to effectively secure cyberspace, or whether four of those sectors – energy, financial services, IT and government services – should be the primary focus of cybersecurity PPP efforts.

[87] Lewis, James A.,"Cybersecurity Two Years Later: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2011, January). http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

The widely varying maturity of ISACs also poses challenges, as does the sheer quantity of government entities with which any one sector needs to partner. As noted previously, several CIKR sectors have yet to stand up ISACs, meaning that the federal government lacks a functioning counterpart for direct information sharing in several industries.[88]

Another continued concern is lack of engagement in cybersecurity PPPs by small and medium-sized entities in both the public and private sectors. Despite efforts by the ISACs to engage the smaller players in their industries – including tiered membership fees and even free access in some cases – ISAC leaders acknowledge that significant barriers exist for small, resource-constrained organizations to participate in such cross-sector partnerships, let alone broader efforts spanning multiple sectors.[89] Most small businesses lack the financial or time resources to focus on external partnerships, particularly in a tough economic environment. In many cases, trade associations constitute the only mechanism for information sharing for small- and medium-sized businesses.[90] This problem extends to local governments as well: of 39,000 local governments in the U.S., only about 200 are currently involved in the MS-ISAC today, despite focused efforts to help create state-level ISACS as a forum for local engagement.[91] This lack of engagement is of particular concern because smaller businesses will be increasingly targeted with cyber attacks as effective information sharing helps to improve the cybersecurity of larger industry players. Thus, while it may be possible to accomplish many of the objectives of

[88] It is possible that the industries which have not yet created ISACs have failed to do so – at least in part – due to the continued disagreement as to whether the participation of their sectors is necessary to securing cyberspace. Industry leaders are unlikely to invest the significant resources necessary to create and support an ISAC without a strong case as to why such an expenditure of resources is necessary. Additionally, this should not be read as suggesting that the federal government is a monolith in the area of cybersecurity. Even the most mature ISACs are faced with the difficult task of coordinating with at least a half dozen federal agencies – putting aside state and local actors – due to the fact that no single federal entity has been designated as the focal point for partnership with the private sector.

[89] Anonymous, personal communication, 2012

[90] Berkeley, A. R. III, Bush, W., Heasley, P. G., Nicholson, J. B., Reid, J. A., Wallace, M. J. Intelligence Information Sharing: Final Report and Recommendations. National Infrastructure Advisory Council. January 10, 2012 http://www.dhs.gov/xlibrary/assets/niac/niac-intelligence-information-sharing-final-report-01102012.pdf

[91] Anonymous, personal communication, 2012

cyber security – such as research and development, building human capital, policy development – without the engagement of smaller players, the effectiveness of information sharing and threat mitigation will always be limited without the participation of smaller entities in both sectors.

Though trust has been built in limited situations, current efforts at cybersecurity PPP have rarely succeeded in building trusted relationships that extend beyond small groups of partners, whether between public and private actors or between actors in a particular sector. This is not necessarily a sign of failure: it may not be possible to build trusted relationships in groups larger than 15 to 30 individuals.[92] In short, building trust within and among partnerships may be the biggest barrier to the work of PPPs seeking to secure cyberspace.

The problem of building trust is magnified when stakeholders between whom trust is needed come to a partnership with misaligned expectations. Those that have succeeded in building effective PPPs have done so by recognizing that government stakeholders usually approach cybersecurity as a public good – and a matter vital to national security – while their private sector counterparts view it as a means to maximize profit by safeguarding intellectual property and other company assets. In a situation where trust is not a given to begin with, these different viewpoints require that each sector be given strong – and often dissimilar – incentives to invest in PPPs that reach beyond the most basic information sharing goals. Thus far, legislative solutions to incentivize voluntary participation – such as reducing private sector liability or offering tax breaks for engagement – have been proposed, but not enacted.

Finally, large gaps persist in the current PPP landscape. It is impossible to judge the progress of PPPs in areas where work has not yet begun. For example, while infrastructure has been built for the purposes of cybersecurity information sharing and, to some extent, policymaking, few PPP structures have been built to address other vital objectives such as

[92] James A. Lewis, in personal communication with the author, February 2012.

research and development, building of human capital,[93] international policy development or altering the architecture of the Internet to create future iterations built with cybersecurity in mind.[94][95][96]

[93] Lewis, James A., "A Human Capital Crisis in Cybersecurity: Technical Proficiency Matters" Center for International & Strategic Studies. (2010, November.) http://csis.org/files/publication/100720_Lewis_HumanCapital_WEB_BlkWhteVersion.pdf

[94] It is possible that parallel PPP tracks have not been built to address the full range of cybersecurity objectives because there is a general consensus that information sharing to identify, mitigate and deter cyber threats is the most pressing of cybersecurity aims. It is equally possible that such efforts have not been undertaken because no one has paid attention to the fact that this gap in the PPP landscape exists (beyond the occasional mention in various academic reports). Indeed, efforts are only now beginning to map out the full scope of PPPs in operation today (Lewis, 2012), let alone to connect the cybersecurity threads that each is following.

[95] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).

[96] Lord, K. & Sharp, T. "America's Cyber Future: Security and Prosperity in the Information Age." Center for a New American Security. (2011, June). Vol. 1 & 2.

REFRAMING CYBERSECURITY PARTNERSHIP

Analysis of existing cybersecurity PPPs in the previous chapter suggests that many of the existing partnerships were borne out of a sense of urgency rather than a systematic analysis of the structures best suited to the particular challenges of securing cyberspace. Given the significant pressure on both public and private entities to share information about cyber threats, it is unsurprising that key stakeholders built upon preexisting relationships, historical connections and organizational structures originally intended for other purposes in fashioning the first generation of cybersecurity PPPs – yielding structures that often reflect expedience rather than thoughtful design. Thus, the success enjoyed by cybersecurity PPPs to date has been achieved – to a great degree – in spite of perceived flaws in partnership design and governance.

With more than a decade of precedent and experience now amassed, the field of cybersecurity policy is sufficiently mature to warrant strategic reflection regarding the model of PPP best suited to accomplish the nation's cybersecurity goals and objectives. Finding that the application of PPP to cybersecurity policy is appropriate, this chapter seeks to reframe the current concept of cybersecurity PPP, examining the fundamentals that should underpin any PPP and considering the unique requirements of a cybersecurity PPP in particular.

THE THEORY OF PARTNERSHIP

PPP is a tool employed in a multitude of policy areas. The popularity of PPP as a tool derives both from the necessity of sector partnership and the significant benefits that a well-designed partnership can yield; among them, increased efficiency and effectiveness, greater

flexibility and stakeholder engagement, innovation and the development of best practices.[9798] A successful partnership increases trust and collaboration, enables shifts in culture and practice, and engages influential supporters to further its goals – ultimately empowering its participants to create value beyond what they could achieve alone.[99]

Regardless of its policy focus, the odds of a partnership succeeding depend largely upon its initial design.[100] PPPs that fail most often do so because of principal-agent problems, stakeholder opposition, ambiguity in professed goals and accountability measures or a lack of resources.[101] In contrast, successful partnerships are characterized by partners with past PPP experience, key leadership support, strong business cases underlying engagement on all sides, clear agreements and aligned missions between partners, consistent oversight and evaluation, and managed risk by all parties.[102]

To ensure success, Goldsmith and Eggers suggest several questions to inform the initial design of any PPP: [103]

- What does the partnership hope to accomplish?
- Which are the most appropriate partners to help the partnership accomplish its goals?
- What design will best suit the partnership, given its professed goals?
- How should the partnership be managed and governed to accomplish those goals?[104]

[97] S. Smith, in personal communication with the author, 2011.
[98] In the case of cybersecurity, the literature is emphatic that cyberspace cannot be secured by one sector alone – that partnership between public and private is vital to this goal.
[99] S. Smith, in personal communication with the author, 2011.
[100] Goldsmith, S., Eggers, W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press (2009).
[101] Ibid.
[102] Ibid.
[103] Goldsmith, S., Eggers, W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press (2009).
[104] Goldsmith and Eggers offer five questions to consider at the start of partnership design. Four of these are relevant for the purposes of this analysis.

APPLICATION OF PARTNERSHIP THEORY TO CYBERSECURITY POLICY

The areas of inquiry suggested by Goldsmith and Eggers provide a beneficial framework through which to determine the fundamental framework of a PPP model best suited to secure cyberspace.[105]

GOALS AND OBJECTIVES

To begin, what must a cybersecurity PPP accomplish? To say that it must secure cyberspace is too vague a goal to make success measurable.[106] Cyberspace must be defined clearly before a PPP can successfully secure it.

The CNCI describes cyberspace as the "interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[107] Unfortunately, the literature is less decisive regarding what it means to secure cyberspace. There is little consensus as to whether cybersecurity means protection against cyber threats, deterrence of attacks, resilience in the face of imminent assaults, or some combination of those objectives.[108] However, PPD-8 offers some clarity on this point, stating that both security and resilience are vital to preparing for the threats that pose the greatest risk to the Nation, including cyber attacks.[109][110]

[105] Goldsmith, S., Eggers, W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press (2009).
[106] Indeed, the lack of clarity around the definition and precise goal of cybersecurity is perhaps a partial explanation for the limited gains that PPPs have made over the past decade.
[107] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).
[108] A review of foundational documents including the 2003 National Strategy to Secure Cyberspace, HSPD-7, the 2008 CNCI (NSPD-54/HSPD-23), the 2011 Cyber Policy Review and the 2011 DOD Strategy for Operating in Cyberspace revealed little consensus as to whether the ultimate goal of cybersecurity efforts should be protection from, deterrence of, or resilience in the face of cyber attacks.
[109] PPD-8 defines these terms as the following: Security is the "protection of the Nation and its people, vital interests, and way of life." Resilience is the "ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies" (White House, March 30, 2011).

PPD-8 further describes the specific importance of building and improving capabilities to "prevent, protect against, mitigate the effects of, respond to, and recover from" cyber threats that pose the greatest risk to national security.[111] This suggests that any comprehensive cybersecurity PPP must have at its core the broad goals of security and resilience, with specific focus on capabilities for prevention, protection, mitigation, response, and recovery.[112]

With these goals in mind, the appropriate objectives to achieve security and resilience – including capabilities for prevention, protection, mitigation, response and recovery – should be clearly defined. Though the bulk of PPP efforts thus far have focused on sharing information to detect and combat cyber threats, both expert commentary and the related literature recommend a much wider set of objectives for which partnership is vital. In addition to information sharing, the spectrum of cybersecurity objectives include coordinated incident response, research and development of superior technological tools to prevent and mitigate cyber threats, technical standard setting to ensure interoperability, the development and coordination of cyber policy at the national and international levels, and the building of sufficient human capital to carry out each of these objectives. This is not to say that the initial focus of cybersecurity PPPs on information sharing has been misplaced: the infrastructure required to effectively share information can ease work toward the other objectives and is thus an appropriate first priority. However, the design of any comprehensive cybersecurity PPP must take each objective into account in order to achieve success on all counts.

---

[110] White House, Presidential Policy Directive 8 on National Preparedness, (Washington, DC: U.S. Government Printing Office 2011).

[111] Ibid.

[112] PPD-8 defines these terms as the following: Prevention refers to those capabilities necessary to avoid, prevent, or stop a threatened or actual act of terrorism. Protection refers to those "capabilities necessary to secure the homeland against acts of terrorism and manmade or natural disasters." Mitigation refers to those "capabilities necessary to reduce loss of life and property by lessening the impact of disasters." Response refers to those "capabilities necessary to save lives, protect property and the environment, and meet basic human needs after an incident has occurred." Recovery refers to those "capabilities necessary to assist communities affected by an incident to recover effectively." (White House, March 30, 2011).

APPROPRIATE PARTNERS

Addressing the second of Goldsmith's inquiries, the design of a comprehensive cybersecurity PPP should be informed by knowledge of the partners most appropriate to accomplish its professed goals. At the most basic level, both public and private sector entities have vested (though varying) interests in cybersecurity and must be engaged. Because leadership support at the highest levels is key to success, public sector engagement should include the White House.[113] To ensure engagement on the full slate of objectives, the public side of the partnership must also include representatives the homeland security, intelligence, military and diplomatic communities. In short, DHS, DOD, DOJ, FBI, NSA and the Department of State must be key partners, represented by a lead agency when appropriate. The engagement of state, local, tribal and territorial government entities across the nation is also important to ensuring the security of critical digital infrastructure at the regional and local levels. Finally, international governments must be engaged – either through inter-governmental channels or directly through PPPs – to ensure the interoperability of both technical and policy solutions.

The sphere of appropriate private sector partners includes both industry and the nonprofit community, with the latter encompassing both academia and advocates for privacy and civil liberties. For example, the involvement of nonprofit organizations focused on Internet governance is imperative to achieving policy coordination, while those focused on technological advancement are vital to fostering research and development in the area of cybersecurity – as are the academic counterparts in either arena.

With regard to industry partners, they should be chosen from the community of private entities owning or managing the type of digital infrastructure deemed a strategic national asset in

[113] S. Smith, in personal communication with the author, 2011.

the President's National Security Strategy.[114] More specifically, private partners should own a "physical or virtual information system that controls, processes, transmits, receives or stores electronic information in any form including data, voice, or video."[115] However, even this narrowed category of digital infrastructure encompasses a vast number of potential industry partners. While experts continue to disagree about which digital infrastructure is "critical," the definition from the Administration's current legislative proposal provides a framework for this analysis.[116] With that context in mind, industry actors should be considered necessary partners only if the digital infrastructure they own or manage is so vital to the nation that its incapacity or destruction would have a debilitating impact on national security, national economic security, or national public health and safety; or if it is owned or operated by or on behalf of a State, local, tribal, or territorial government entity.[117] By this definition, partners will include entities from a host of industries – in particular, the eighteen CIKR sectors identified by DHS has identified as CIRK sectors.[118] It is equally important that private sector partners include industry entities of varying size, from the largest corporations to those still in startup mode.

DESIGN SUITED TO GOALS

The goals, objectives and partners deemed necessary and appropriate for a cybersecurity PPP will inform its design. While the long roster of necessary partners provides goalposts for the design, the incentives required to drive partner engagement will shape the internal workings of a partnership.

[114] White House, National Security Strategy, (Washington, DC: U.S. Government Printing Office, 2010).
[115] Department of Homeland Security. Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise. (Washington, DC: GPO, November 2011)
[116] Ibid.
[117] Ibid.
[118] Ibid.

Differing motivations for partnership mean that public and private sector actors are unlikely to partner successfully without effective dialogue to build understanding between the two sets of actors. Thus, trust building is vital in developing true partnership. However, trust is not enough: incentives must also be properly aligned to reward each sector for their engagement. An incentive-based approach is best accomplished by tying incentives to results rather than activities.[119] By clearly establishing an end goal, partners can more easily overcome cultural differences, achieving success even while working toward it in very different manners.

As discussed in relation to key institutions, the incentives that drive engagement by public sector partners are fundamentally different from those motivating the private sector. Put simply, government stakeholders appear to approach cybersecurity as a matter of national security – they require information and expertise from private sector entities in order to secure cyberspace effectively and thus, consider partnership a public good. In contrast, their private counterparts appear to view cybersecurity as a necessary expenditure in order to safeguard investments in intellectual property and other assets. Partnership with the public sector is of interest only to the extent that it furthers the goal of maximizing profit. The experiences of DCISE and ICASI are illustrative of the incentives likely to drive private sector engagement: in each case, private sector actors have called for such partnerships to provide access to innovative security products, as well as the ability to maintain a level of privacy from government partners – whether for liability or competitive concerns – through anonymized reporting. A properly incentivized PPP will offset the challenges raised by competitive and liability concerns and mitigate the inclination to withhold information.

[119] Goldsmith, S., Eggers, W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press (2009).

Within the full complement of partners necessary for a successful cybersecurity PPP, certain individual actors will not be compatible in one-to-one relationships. Their fundamentally misaligned perspectives and incentives will make it difficult, if not impossible, to engage directly in a fruitful partnership. Similarly, entities that are competitors in the same functions where they are asked to partner – especially when those areas of cooperation are core to each entity's business model – will be likely unwilling to share the proprietary information necessary to advance research and design objectives, or to inform the creation of best practices and policy positions.[120] Therefore, the design of the partnership itself must seek to form direct connections where they will be fruitful, and to moderate collaboration between individual partners where direct connection would prove counterproductive.

Further, while the support of senior leaders from each sector is vital, it is equally important that partnership extend to the tactical levels within partner organizations in order to ensure that the most nuanced engagement occurs between experts at any rank. Thus, any partnership must allow for connection among senior officials, and between those working at a tactical level in various partner entities.

GOVERNANCE AND MANAGEMENT

The question of who should govern a cybersecurity PPP is much debated. The literature is inconclusive on the subject of whether the federal government should hold ultimate authority over the partnership, whether a third party (such as a nonprofit) would be best suited to facilitate all partners reaching their shared goal, or whether a centralized governing mechanism is necessary at all.

[120] Ibid.

While much of the current debate focuses on public versus private control, the most appropriate model of governance depends foremost on the balance of flexibility and accountability desired in the partnership. A partnership driven primarily by a need for accountability will require more rigid infrastructure (and perhaps a contractual network of sorts) whereas a partnership valuing flexibility will be better suited by a looser framework.[121]

Given that cybersecurity is a matter of national security, it might seem logical to value accountability above flexibility in the design of a related PPP. However, the fast-evolving nature of cyber threats, and the need for rapid technological advancement to address such challenges, makes flexibility extremely important in a cybersecurity PPP. This does not preclude regulatory mechanisms to encourage an environment in which partners are held accountable for their activities, but the structure of the PPP itself must be flexible enough to meet its objectives as cyberspace evolves.

[121] Ibid.

IDENTIFICATION AND ANALYSIS OF ALTERNATIVES

As previously discussed, the goal of this paper is to determine the model of PPP best suited to secure cyberspace. This chapter proposes and analyzes four PPP alternatives in order to identify the most appropriate alternative for implementation. A survey of the current cybersecurity PPP landscape – coupled with models being proposed in legislation – provides several strong alternatives to consider.

IDENTIFICATION OF ALTERNATIVES

The status quo – the current landscape of PPPs relying on voluntary engagement by both private and public sector actors – should be the first alternative evaluated to determine whether any change is necessary to achieve the nation's cybersecurity goals. This first alternative was discussed in detail in previous chapters. Because they were designed specifically with the goal of improving cybersecurity through PPP, legislative proposals to create a National Information Sharing Organization and a cybersecurity exchange will be discussed and evaluated as two separate alternatives.[122][123] Finally, a fourth alternative informed by Goldsmith and Eggers' fundamental considerations for PPP design will be proposed and evaluated. This fourth alternative proposes the implementation of two "civic switchboards" – a concept that will be discussed in detail later in this chapter – to improve the efficacy of existing PPPs, rather than the creation of a new PPP.[124] While the status quo has been discussed in detail in the previous chapter, the fundamentals of the other three alternatives are set forth below.

[122] H.R. 3674 111th Cong., (2011)
[123] S. 2105, 112th Cong., (2012).
[124] A civic switchboard is a model of partnership introduced by Stephen Goldsmith in which the government or another appropriate entity "uses its broader perspective to connect diverse organizations in a manner where they augment each other's capacity to produce an important public outcome." In a civic switchboard, the coordinating

NATIONAL INFORMATION SHARING ORGANIZATION

One cybersecurity legislative proposal considered in the 112th Congress would significantly change the existing PPP landscape, creating a National Information Sharing Organization (NISO). As envisioned in the "Promoting and Enhancing Cybersecurity and Information Sharing Effectiveness (PRECISE) Act of 2011", introduced by Representative Dan Lungren (D-CA 3), the NISO would be a non-profit organization serving as a national clearinghouse through which public and private actors could exchange cyber threat information such that the owners and operators of networks or systems would have "access to timely and actionable information in order to protect their networks or systems as effectively as possible."[125]

As described in the bill, the objectives of the NISO would be information sharing regarding cyber threats, the exchange of technical assistance, advice and support," and the development and dissemination of security technology necessary to secure cyberspace.[126] The NISO would also engage in research and development projects to improve cybersecurity in CIKR sectors, increase transferability and use of intellectual property; and integrate with the federal government through the NCCIC.[127]

As introduced, the PRECISE Act of 2011 noted that the NISO could be chosen from existing organizations or partnership structures, but that it is intended to create one "common operating picture" by combining cyber threat warning information and sharing it through an automated mechanism.[128] The bill called for the NISO to be governed by a board including a DHS representative, four representatives from three federal agencies with cybersecurity

---

entity "brings a unique perspective that can be used to connect civic organizations that provide a service, but are in need of resources, with others who might have that resource" (Goldsmith & Eggers, 2009).

[125] H.R. 3674, 112th Cong., 1st Sess. (2011)

[126] Ibid.

[127] Ibid.

[128] Ibid.

responsibilities, ten representatives from the private sector, two representatives from the privacy and civil liberties community, and the chair of NCI.

The NISO alternative would constitute a significant change from the current "status quo" in which public and private entities partner voluntarily and with limited coordination between individual PPP efforts. The creation of a NISO would require existing PPPs focused on the objectives of information sharing, incident response, and research and design, to reorient their efforts in such a way as to be integrated into the NISO clearinghouse – which would serve as the primary PPP for these objectives – in order to remain relevant to the broader goals of cybersecurity.

It is unclear whether the creation of a NISO would go even farther, replacing entirely the type of information sharing currently taking place in the ISACs and SCCs. In testimony before the U.S. House of Representatives Committee on Homeland Security in December 2011, Gregory T. Nojeim of the Center for Democracy & Technology cautioned against creating a new PPP that would turn out not to address the deficiencies of those already working to secure cyberspace,[129] while Cheri F. McGuire of Symantec Corporation warned against undermining existing efforts such as the ISACs and SCCs, in which significant time and resources have already been invested.[130]

CYBERSECURITY EXCHANGE

The "Cybersecurity Act of 2012," introduced by Senators Joe Lieberman (D-CT), Susan Collins (R-ME), Jay Rockefeller (D-WV), and Dianne Feinstein (D-CA) during the 112th

[129] Draft Legislative Proposal on Cybersecurity: Hearing before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, 112th Cong (2011) (Statement of Gregory T. Nojeim

[130] Draft Legislative Proposal on Cybersecurity: Hearing before the U.S. House of Representatives Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies, 112th Cong. (2011) (Statement of Cheri F. McGuire).

Congress, would require the federal government to designate an agency or office as the lead "cybersecurity exchange" to serve as the focal point within the federal government for sharing among "federal and non-federal entities." [131]Like the NISO alternative, the cybersecurity alternative would require existing PPPs to reorient their efforts significantly in order to align with the identified cybersecurity exchange, which would act as the primary PPP over others working toward the objective of information sharing. Rather than connecting directly with appropriate federal agencies in partnerships tailored to the particular partners' needs regarding information sharing, private sector partners would be required to work through this new cybersecurity exchange in order to collaborate with public partners.

While another entity could later be designated, the Cybersecurity Act of 2012 (as introduced) identified the NCCIC as the "interim" body to serve as the lead cybersecurity exchange from the point at which the bill is enacted into law. The lead cybersecurity exchange would be responsible for receiving and distributing cybersecurity threat indicators; facilitating information sharing, interaction, and collaboration among and between public and private actors; and disseminating timely and actionable cybersecurity threat, vulnerability, mitigation, and warning information. The lead cybersecurity exchange would be the primary nexus for cybersecurity coordination between Federal entities; state, local, tribal, and territorial governments; academia; international partners; and all aspects of the private sector. The bill also allowed for the creation of other cybersecurity exchanges, but requires that they be federal entities.[132]

In testimony before the Senate Homeland Security and Government Affairs Committee, Senator Feinstein stated that the cybersecurity exchange is intended to "serve as a hub for

[131] S. 2105, 112th Cong., (2012).
[132] S. 2105, 112th Cong., (2012).

appropriately distributing and exchanging cyber threat information between the private sector and the government," but did not elucidate other objectives beyond information sharing.[133] During the same hearing, Tom Ridge cautioned in his testimony against the creation of new regulatory structures before the private and public sectors have "done nearly everything they can within the public-private partnership framework."[134]

CIVIC SWITCHBOARDS

With the multitude of goals, objectives and partners necessary to secure cyberspace – and the number of existing PPP efforts already achieving some level of success – reliance on a new, unified partnership may not be sufficient to achieve success on all counts. Thus, the fourth alternative proposed is not itself a new PPP. Instead, the proposal is to implement a set of two "civic switchboards" – each focused on a subset of the necessary cybersecurity goals and objectives – to improve the functioning of the existing PPP landscape.

A civic switchboard is a model of partnership introduced by Stephen Goldsmith in which the government or another appropriate entity "uses its broader perspective to connect diverse organizations in a manner where they augment each other's capacity to produce an important public outcome."[135][136] In a civic switchboard, the coordinating entity "brings a unique

[133] "Securing America's Future: The Cybersecurity Act of 2012," US Senate Committee on Homeland Security and Government Affairs, February 16, 2012, Last Accessed: August 16, 2013, http://www.hsgac.senate.gov/hearings/securing-americas-future-the-cybersecurity-act-of-2012.

[134] Ibid.

[135] The concept of a "civic switchboard" was first introduced and implemented by Stephen Goldsmith in 1997 during his time in office as the mayor of Indianapolis. The concept is discussed briefly in The Twenty-First Century City: Resurrecting Urban America, published by Goldsmith in 1999. The concept is described in greater detail in Governing by Network: The New Shape of the Public Sector, published by Goldsmith with William D. Eggers in 2009. The latter work is cited throughout this paper.

[136] Goldsmith, S., Eggers, W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press (2009).

perspective that can be used to connect civic organizations that provide a service, but are in need of resources, with others who might have that resource."[137]

When viewed in the context of the broad continuum along which public-private collaboration occurs – from tightly structured contractual relationships to highly integrated and interdependent networks – civic switchboards require the lowest level of direct government control.[138][139] In some cases, the government need not engage in the partnership at a tactical level, instead simply facilitating the creation of a civic switchboard that can connect the resources of necessary partners such that they can achieve those goals directly.

In this case, the fourth alternative would create one government-coordinated civic switchboard to focus on objectives requiring direct government coordination, and a second nonprofit-coordinated civic switchboard to focus on the objectives not requiring government leadership. Unlike the NISO or cybersecurity exchange alternatives, the dual civic switchboards would not function as new PPPs exerting primacy over other existing PPPs. Instead, each civic switchboard would simply work to enhance and better connect the individual PPP efforts focused on their identified objectives, and to foster best practices across the entire PPP landscape.

A government-coordinated civic switchboard would be established to maintain awareness and enhance the efforts of PPPs on information sharing and incident response. Because of the public good inherent in information sharing and incident response, it is appropriate that the government be the convening body for the switchboard focused on those two objectives,

[137] Ibid.
[138] Ibid.
[139] S. Smith, in personal communication with the author, 2011.

facilitating connections between those PPPs in order to better leverage their individual activities in both areas.[140]

In the case of the remaining objectives – research and development, technical standard setting, national and international policy development, and the building of human capital – direct facilitation by the government is not necessary in order to achieve success. Thus, a nonprofit-coordinated civic switchboard would be established to maintain awareness of PPP efforts related to each of these objectives, amplify the impact of their individual efforts, and encourage new PPP on underserved objectives.

ANALYSIS OF OUTCOMES

In order to recommend the model of PPP best suited to secure cyberspace, this section sets forth the appropriate criteria against which to judge each alternative, and examines the outcomes of that analysis.

Each alternative was evaluated against four criteria. The best alternative should:

- Focus on the identified goals;
- Address each of the necessary objectives;
- Engage all necessary partners effectively; and
- Employ a governance structure properly balancing flexibility and accountability.

Ideally, the chosen alternative should have security and resilience as its central goals, building capacity for prevention, protection, mitigation response and recovery from cyber threats. It should address all of the objectives necessary to achieve cybersecurity, including information sharing, incident response, research and development, technical standard setting, the development of relevant policy on the national and international levels; and the building of human capital necessary to achieve the other goals and objectives. The chosen alternative should

[140] Paul Rosenzweig, "Cybersecurity and Public Goods," Hoover Institute (2011), Last Accessed: August 16, 2013 http://media.hoover.org/sites/default/files/documents/EmergingThreats_Rosenzweig.pdf.

engage all of the partners previously identified as necessary in an effective manner: building trust among them; employing properly aligned incentives tied to results; structuring interaction among partners in the most beneficial manner – either directly or indirectly – and connecting counterparts within partner organizations at both strategic and tactical levels. Finally, the best alternative should employ a model of governance that strikes the appropriate balance between flexibility and accountability: one that is loose enough to flexibly address fast-evolving cyber threats and using regulatory mechanisms to create an environment in which partners are held accountable for the effectiveness of their activities, rather than to mandate those actions.

A scale of one through three was assigned by the author to assess the outcomes when each alternative was evaluated against the chosen criteria. An alternative received a score of one when it failed to meet a particular criterion. A score of two was given when an alternative partially met a criterion, and a score of three was given when an alternative fully met a criterion. Because each criterion was deemed equally vital to the success of a public-private partnership that would effectively secure cyberspace, the four criteria were weighted equally.

Table 1: Outcomes Projected for Identified Alternatives

	Alternatives			
Criteria	**Status Quo**	**NISO**	**Cybersecurity Exchange**	**Civic Switchboards**
Focuses on appropriate goals	2	3	2	3
Addresses all necessary objectives	2	2	1	3
Engages all necessary partners effectively	2	1	2	3
Employs balanced governance structure	2	2	2	2
Outcomes	**8**	**8**	**7**	**11**

When evaluated against the criteria deemed vital for a cybersecurity PPP to be successful, the civic switchboard alternative outperformed each of the other alternatives considered (see Table 1).

The landscape of cybersecurity PPPs that make up the status quo collectively focus on both security and resilience, but place much greater emphasis on protection and mitigation response than on prevention and recovery from cyber threats. While there are limited partnership activities in the areas of research and development, technical standard setting, and the development of relevant domestic policy, the efforts of existing PPPs are heavily weighted toward information sharing and incident response. With regard to engaging necessary partners effectively, cybersecurity PPPs have managed thus far to build trust in small groups, but not on a larger scale. They have also failed to adequately engage smaller industry players who should be included as partners. Only a handful of smaller partnerships have employed incentive-based approaches and none of the identified partnerships tie those incentives to results, as opposed to activities. Finally, while the current landscape is sufficiently flexible to address fast-evolving cyber threats, it is likely too loose to hold partners accountable for the effectiveness of their activities.

The NISO alternative is focused on both security and resilience; the information clearinghouse envisioned in the PRECISE Act would help to protect against cyber threats, while the exchange of technical assistance – as well as the development and dissemination of technology – would help to build capacity for prevention, mitigation and recovery. Through those mechanisms, the NISO addresses the objectives of information sharing, incident response and research and design, but fails to address the three remaining objectives. As described in the PRECISE Act of 2011, the NISO would not engage all necessary partners in an effective manner

as it does not include mechanisms for building trust, incentivizing partner engagement, structuring interaction between partners, or connecting counterparts at tactical levels, instead relying solely on a governing board that puts public and private partners with potentially competing interests at the same table. It also fails to ensure that both large and small entities are engaged. Though the NISO alternative is threat-neutral and so could remain a useful forum for information sharing and technology development as cyber threats evolve, it stops short of holding partners accountable for the effectiveness of their actions.

The cybersecurity exchange alternative would adequately focus on the goal of security – facilitating information sharing related to threats, vulnerabilities and mitigation – but would not include resilience as a central goal, making it unlikely to build capacity related to prevention or recovery. Further, it is designed with the sole objective of information sharing: while improved incident response might result from the sharing of information about mitigation strategies, incident response is not a stated objective, and the alternative fails to address any of the other four objectives. As envisioned in the Cybersecurity Act of 2012, the cybersecurity exchange alternative would function through NCCIC – at least to begin in the early stages. It is assumed, therefore, that the alternative would engage partners with an equal level of success as NCCIC has achieved to date. Given that assumption, the cybersecurity exchange alternative would likely employ effective incentives and build trust among the partners that it did engage, but there is no reason to believe that it would engage smaller partners, or the nonprofit community. Further, the NCCIC floor does not provide sufficiently structured interaction among partners, connecting them all directly on the floor at a tactical level, but failing to engage those same partners at the strategic level to meet objectives beyond information sharing and incident response. Like the NISO, the cybersecurity exchange alternative (NCCIC) is threat-neutral and so could remain a

useful forum for information sharing and technology development as cyber threats evolve, but it stops short of holding partners accountable for the effectiveness of their actions.

The civic switchboards alternative would focus on all of the appropriate goals to secure cyberspace by virtue of connecting and amplifying the work of existing PPPs (which collectively, if not individually, focus on both security and resilience, building capacities for prevention, protection, mitigation response and recovery from cyber threats). Using civic switchboards would address all of the objectives necessary to achieve cybersecurity, including information sharing, incident response, research and development, technical standard setting, the development of relevant policy on the national and international levels; and the building of human capital necessary to achieve the other goals and objectives. By connecting existing PPPs, the civic switchboards would build trust across partners and partnerships, amplifying the trust that individual PPPs have already built within their smaller groups. While the civic switchboards would not employ incentives directly tied to results, their work in raising awareness of PPPs that are successfully employing results-based incentives is likely to result in those best practices being adopted more widely, while also bringing attention to less successful PPPs and increasingly the likelihood that those efforts will eventually fall away for lack of quantifiable results. The nature of the civic switchboards allows for partners to be connected directly or for their work to be indirectly leveraged by the switchboards, depending on which approach is most appropriate in a particular situation. Similarly, the civic swithcboards can connect counterparts within partner organizations at both strategic and tactical levels, as is appropriate. Finally, the model of governance seen in the civic switchboard alternative – connecting partners formally or informally over time depending on their areas of focus and the needs of the larger cybersecurity community – is flexible enough to adapt as cyber threats and technology continue to evolve.

Though the civic switchboard alternative does not enable the civic partnerships to regulate the PPPs in the cybersecurity community, it does foster accountability through self-regulatory means, raising awareness of best practices and bringing focus to results-based efforts.

Table 2: Discussion of Outcomes Projected for Identified Alternatives

Criteria	*Alternatives*			
	Status Quo	**NISO**	**Cybersecurity Exchange**	**Civic Switchboards**
Focuses on appropriate goals	**2 –** Focuses on both security and resilience, but places much greater emphasis on protection and mitigation response than on prevention and recovery from cyber threats.	**3 –** Focuses on both security and resilience. Would help to protect against cyber threats, and help to build capacity for prevention, mitigation and recovery.	**2 –** Focuses on the goal of security. Does not include resilience as a central goal, making it unlikely to build capacity related to prevention or recovery.	**3 –** Focuses on all appropriate goals. Amplifies focus of existing PPPs on both security and resilience. Increases focus on building capacities for prevention, protection, mitigation response and recovery from cyber threats.
Addresses all necessary objectives	**2 –** Activity heavily weighted toward information sharing and incident response, with limited focus in the areas of research and development, technical standard setting, and the development of relevant domestic policy.	**2 –** Addresses the objectives of information sharing, incident response and research and design. Fails to address the three remaining objectives.	**1 –** Designed with the sole objective of information sharing. Improved incident response might result from the sharing of information about mitigation strategies, but is not a stated objective. Fails to address any of the other four objectives.	**3 –** Addresses all necessary objectives.
Engages all necessary partners effectively	**2 –** Builds trust in small groups, but not on a larger scale. Fails to adequately engage smaller industry players who should be included as partners. Makes limited use of incentive-based approaches. Fails to tie incentives to results.	**1 –** Does not include mechanisms for building trust, incentivizing partner engagement, structuring interaction between partners, or connecting counterparts at tactical levels. Puts partners with potentially competing interests at the same table. Fails to ensure that both large and small entities are engaged.	**2 –** Employs effective incentives and build trust among the partners that are engaged. Does not engage smaller partners, or the nonprofit community. Does not provide sufficiently structured interaction among partners. Connects partners at tactical level, but not at the strategic level to meet objectives beyond information sharing and incident response.	**3 –** Builds trust across partners and partnerships, amplifying trust build in existing PPPs. Indirectly employs incentives tied to results. Allows partners to be connected directly or for their work to be indirectly leveraged by the network. Connects partner organizations at both strategic and tactical levels.
Employs balanced governance structure	**2 –** Employs governance model sufficiently flexible to address fast-evolving cyber threats, but likely too loose to hold partners accountable for the effectiveness of their activities.	**2 –** Employs governance model flexible enough to adapt as cyber threats and technology continue to evolve. Fails to hold partners accountable for the effectiveness of their actions.	**2 –** Employs governance model flexible enough to adapt as cyber threats and technology continue to evolve. Fails to hold partners accountable for the effectiveness of their actions.	**2 –** Employs governance model flexible enough to adapt as cyber threats and technology continue to evolve. Fosters accountability through self-regulatory means, raising awareness of best practices and bringing focus to results-based efforts.
Outcomes	**8**	**8**	**7**	**11**

RECOMMENDED STRATEGY FOR IMPLEMENTATION

PPP is a vital tool to achieve the national priority of securing cyberspace.[141] As noted in previous chapters, a host of cybersecurity PPPs are already in operation today. However, the status quo, NISO and cybersecurity exchange alternatives proposed fail to meet all of the criteria necessary in a PPP that will effectively secure cyberspace. The best alternative calls for the creation of a set of two civic switchboards – a tool through which the government or another appropriate entity "use its broader perspective to connect diverse organizations in a manner where they augment each other's capacity to produce an important public outcome."[142] This chapter outlines a recommended strategy for the implementation of one government-coordinated civic switchboard and one nonprofit-coordinated civic switchboard to improve the efficacy of existing cybersecurity PPPs by connecting partnerships and better leveraging their work across the full spectrum of goals and objectives necessary to secure cyberspace.

GOVERNMENT-COORDINATED SWITCHBOARD

As discussed in previous chapters, the inherent public good derived from information sharing and incident response makes it appropriate that government should have a direct role in coordinating the civic switchboard focused on coordinating PPPs around those cybersecurity objectives.

In order to ensure that it has the proper perspective and authority with which to view and optimize PPP efforts in these areas, management of the government-coordinated switchboard should reside in the Executive Office of the President. Though DHS is the lead agency

[141] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).
[142] Goldsmith, S., Eggers, W. D. Governing by Network: The New Shape of the Public Sector. Washington, DC: Brookings Institution Press (2009).

responsible for working with the private sector to secure cyberspace and America's cyber assets, only the White House has direct oversight and authority over the full gamut of government agencies that must be engaged in such partnerships.[143] This proposed organizational structure and mission are in line with the near-term actions identified in the President's Cybersecurity Policy Review, which called for the President to designate cybersecurity as one of his key management priorities and to establish related performance metrics; and to prepare a cybersecurity incident response plan and initiate dialog to enhance public-private partnerships. [144] Thus, given that the President has created a Cybersecurity Office – part of the national security staff within the Executive Office of the President – to take such actions, it is the most appropriate office to oversee the coordination of switchboard activities relating to information sharing and incident response, in addition to its existing responsibilities.

For the Cybersecurity Office to manage the government-coordinated civic switchboard effectively will require staff with expertise in partnership design and function as well as cybersecurity policy. The wealth of existing nonprofit organizations focused on cybersecurity partnership – in particular, the network of ISACs – as well as the academic community might provide a pool of qualified candidates with such expertise.

In creating the government-coordinated civic switchboard, the first objective of the Cybersecurity Office should be to map the existing environment of cybersecurity partnerships focused on information sharing and incident response. This initial survey would determine the full landscape of partnerships – whether public-private, private-private or public-public – working in this area such that the switchboard staff can later examine each partnership more

[143] "Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency." Center for International & Strategic Studies. (2008, December.) http://Csis.org/media/pubs081208_securingcyberspace_44.pdf.

[144] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).

closely in determining where best practices lie, what connections have already been made between partners, and what efficiencies can be achieved through the switchboard by connecting various efforts.

The survey would also identify key partners not yet engaged in partnerships, providing a list of targets for their outreach to the private sector – a second important function of the switchboard. In addition to understanding the full breadth of work being done through cybersecurity PPPs (around these two objectives) and making direct connections between them as needed, the switchboard staff should also function as a one-stop shop for organizations to learn about PPP efforts and find an easy avenue for engagement. The switchboard can provide particular value to small and medium-sized organizations that need assistance in making the PPP connections most likely to maximize their limited resources.

In line with the 2009 Cybersecurity Policy Review's call to establish related performance metrics, the government-coordinated switchboard should use the knowledge gained by surveying the landscape of PPPs to understand the success metrics currently being used in partnerships and to provide a forum for the creation of standard metrics across the environment. Because the government-coordinated switchboard is not engaged directly in partnership itself, it can serve as a neutral party to broker conversations between partners as to the most appropriate and effective metrics that should guide their collective work. Additionally, the switchboard should work to raise awareness of PPPs that are already successfully employing results-based incentives in their work, amplifying best practice examples for adoption across the cybersecurity landscape.

NONPROFIT-COORDINATED SWITCHBOARD

Achieving success on the remaining cybersecurity objectives – research and development, technical standard setting, national and international policy development, and the

building of human capital – does not require direct facilitation by the government. A nonprofit-coordinated civic switchboard can successfully develop and maintain awareness of partnership efforts related these four objectives, as well as to facilitate connections among partnerships and to amplify the impact of their efforts. Thus, a new entity – possibly called the Partnership for American Cybersecurity Engagement (PACE) – should be established to carry out these functions.

While continued government management is neither necessary nor appropriate, the federal government would likely need to take part in the creation of this nonprofit switchboard to ensure that it has credibility among both public and private partners once established. Again, this mirrors several of the near-term objectives identified in the Cybersecurity Policy Review, which calls for the President to initiate national awareness and education campaign to promote cybersecurity; to develop an international cybersecurity policy framework an strengthen international partnerships; and to develop research and development strategies.[145] These actions are best accomplished by employing the White House Cybersecurity Office to foster work in these areas by the private sector, leaving the Obama Administration (and future administrations) greater resources to focus on the objectives that it must coordinate itself. Thus, this is another role for the Cybersecurity Office to play once it has successfully created the government-coordinated civic switchboard for information sharing and incident response: convene key partners, obtain buy-in across the landscape, and coordinate the resources necessary to launch a new nonprofit, before stepping back to let that private organization facilitate coordination around its desired objectives on an on-going basis.

[145] White House, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure, (Washington, DC: U.S. Government Printing Office, 2009).

The Obama Administration has already been successful in fostering the creation of several nonprofit civic switchboard-like entities to facilitate partnership on various policy objectives. For example, the nonprofit Startup America Partnership (SAP) was convened at the behest of the White House to advance the President's broader "Startup America" economic policy initiative aimed at fostering high-growth entrepreneurship across the country (White House, 2012c). Serving as the point agency for public-private partnership in this area, the Small Business Administration convened private sector partners to create SAP as a private sector counterpart in a PPP. Once SAP was up and running, the SBA stepped back to allow the nonprofit to coordinate directly private sector action to promote entrepreneurship. To date, SAP has assembled more than $1 billion in commitments from dozens of private sector partners to support the growth of startups.[146] Change the Equation is another nonprofit organization that was convened specifically to focus on mobilizing the private sector to improve the quality of science, technology, engineering and math (STEM) education in the U.S., in the service of the Administration's broader "Educate to Innovate" policy initiative to increase STEM literacy.[147]

The Cybersecurity Office should use the same model to foster the creation of PACE, before stepping back to let it coordinate among PPPs and promote engagement by key partners on each of the desired objectives. As in the case of the SAP, the White House – through the Cybersecurity Office – should lead efforts to convene the private sector stakeholders needed to start PACE, but should also solicit input and, in some cases, direct participation from other agencies that have expertise related to each of the objectives that PACE would be tasked to accomplish. For example, the State Department must be consulted in relation to international

[146] "Start-up America," whitehouse.gov, Last Accessed: August 19, 2013, http://www.whitehouse.gov/economy/business/startup-america.

[147] Change the Equation. (n.d.). Our Mission and Goals. Retrieved from http://www.changetheequation.org/our-mission-and-goals.

policy; the Office of Science and Technology Policy (OSTP) with regard to research and development; and the Department of Education (DOE), Department of Labor (DOL) and Office of Personnel Management (OPM) with respect to building human capital. Further, the engagement of these agencies from the start would also provide the new entity, PACE, with direct public sector relationships that it can call upon in its work once it is up and running as a nonprofit organization.

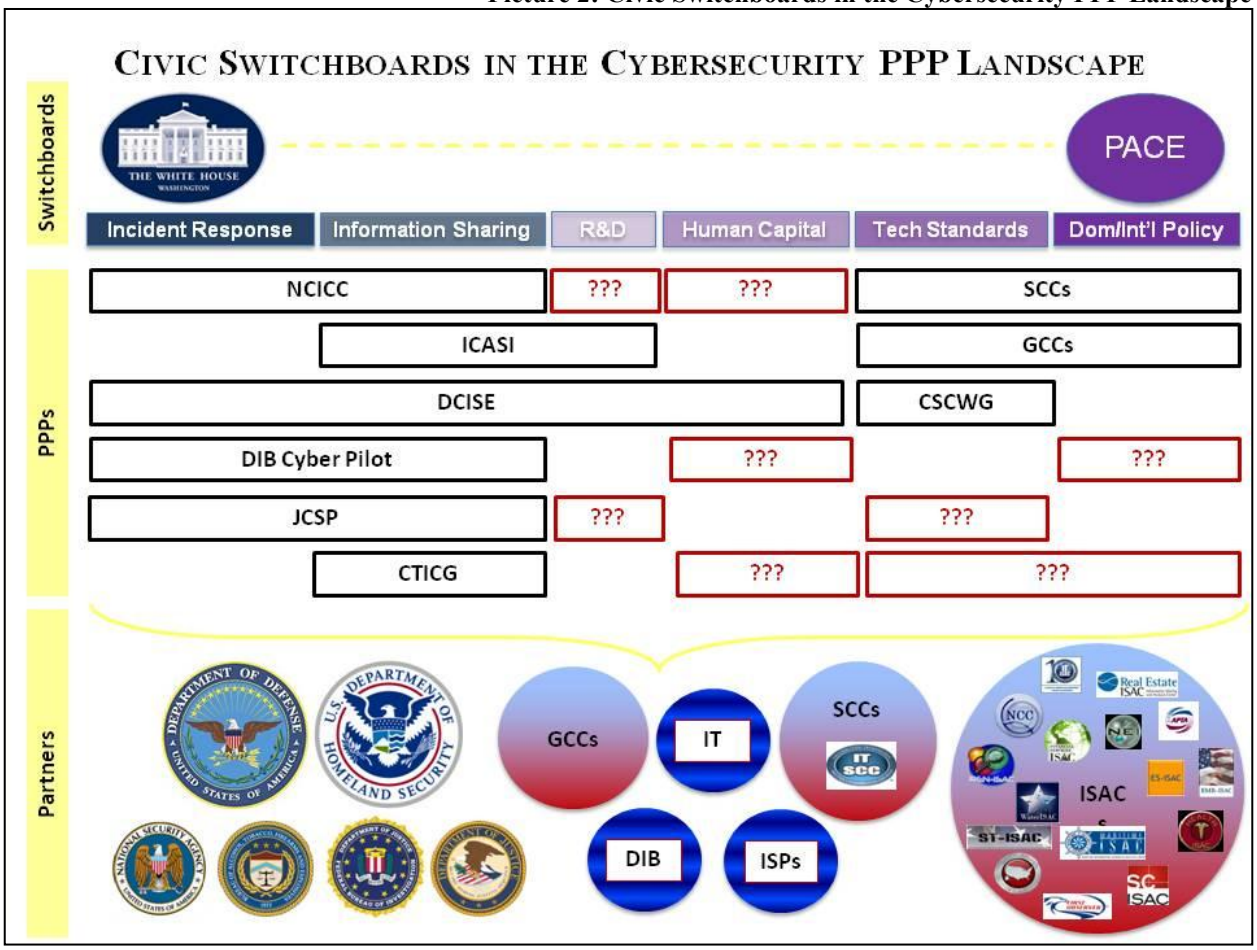
Once PACE is a functioning nonprofit, it should first turn its attention to mapping the full landscape of partnerships involved in achieving the four cybersecurity objectives upon which it is focused. This would be very similar to the mapping exercise undertaken by the Cybersecurity Office on the two key objectives of the government-coordinated civic switchboard.

Beyond mapping the PPP landscape, PACE should put its initial efforts toward closing gaps in the PPP landscape – particularly given that PPP efforts focused on PACE's four cybersecurity objectives remain spotty to date. It should work to promote partnership on underserved objectives, whether by connecting existing PPPs to better leverage their efforts, or by fostering the creation of new PPPs to work in these areas. In some cases, PACE may need to serve as an intermediary between PPPs or individual partners that are unwilling or unable to work together directly, promoting awareness of what others are accomplishing toward a particular objective and providing a conduit for sharing between such efforts. With regard to existing PPPs, PACE should but a particular focus on connecting counterparts within partner organizations at the tactical levels, where those working on cybersecurity objectives are least likely to be aware of and seek to leverage the efforts of others working toward similar ends.

Like its government-coordinated counterpart, PACE should provide a neutral forum for the creation and adoption of success metrics related to each of its objectives. Additionally, it

should amplify awareness of best practices across the PPP landscape. These two functions would likely prove even more vital for PACE, which is focused on objectives where PPP efforts are less fully developed and thus less likely to have reached a point of developing metrics or codifying best practices.

Picture 2: Civic Switchboards in the Cybersecurity PPP Landscape



Sources: Numerous, including Goldsmith & Eggers; ISAC Council; Center for Internet Security; Department of Defense Cyber Crime Center; DHS website; DHS Privacy Impact Assessment for the National Cyber Security Division Joint Cybersecurity Services Pilot; and White House Cyberspace Policy Review.

REGULATION TO ENHANCE CIVIC SWITCHBOARDS

As discussed in previous chapters, the proliferation of PPPs focused on securing cyberspace over the past decade suggests that legislation is not necessary to require that public

and private entities work with one another in partnerships. However, legislation could help create a regulatory environment more conducive to voluntary partnership.

In particular, measures to reduce private sector liability for sharing information with government entities, or with other private sector entities, would remove perceived legal barriers that may be inhibiting PPP participation by private partners of all sizes and across many industries. Similarly, measures clarifying the authority that various federal agencies have to aid the private sector in the case of cyber intrusions would enable such agencies to respond better to requests in a timely manner such that private entities are more likely to see value in partnership.

The White House put forth a cybersecurity legislative proposal in May 2011 that addresses both private sector liability and DHS authority.[148] The proposal would clarify both DHS's authority to help private sector entities experiencing cyber attacks, as well as the type of assistance it can provide. It would give private sector entities immunity from liability in the course of sharing information about cyber attacks, particularly regarding Freedom of Information Act (FOIA) requests that could force the government to make public information about a cyber attack, leaving the attacked company vulnerable to reputational harm or stock price volatility. Similar proposals were made through bipartisan efforts in the 112th Congress, though none were passed into law before the close of the session.[149]

Though legislation proposing each of these enhancements to the regulatory environment has been introduced, continued partisan disagreement over the broader approach to federal

[148] "FACT SHEET: Cybersecurity Legislative Proposal," whitehouse.gov, May 12, 2011, Last Accessed: August 16, 2013, http://www.whitehouse.gov/the-press-office/2011/05/12/fact-sheet-cybersecurity-legislative-proposal.

[149] One such example is the Cyber Intelligence Sharing and Protection Act, H.R. 3523. The act would clarify and expand the intelligence community's ability to share cyber threat intelligence with private sector entities. It would also clarify the actions that a private sector entity experiencing a cyber attack can take to protect its own cyber assets – including sharing information with federal agencies and other private entities – while prohibiting the use of such information to gain competitive advantage, and exempting it from public disclosure (i.e., not subject to FOIA requests). The proposal would also prohibit civil or criminal action against private entities that are engaged in such actions to protect their cyber assets, providing an incentive for the private sector to focus on cybersecurity and to engage in related public-private partnerships.

cybersecurity legislation makes it unlikely that such enhancements would be made in the short term. Should Congress succeed in passing such legislation in the future, it would no doubt improve the environment in which the Cybersecurity Office and PACE work, but neither would the lack of congressional action inhibit either switchboard from succeeding in its objectives in the meantime.

CONCLUSION

This paper asked a foundational question: what model of PPP is most appropriate for the task of securing cyberspace? It presented the findings of the related research before proposing and analyzing four PPP alternatives. In this context, the civic switchboard alternative was identified as the best option for implementation. Finally, a recommended strategy was outlined to guide the implementation of one government-coordinated civic switchboard and one nonprofit-coordinated civic switchboard. Together, these civic switchboards are designed to improve the efficacy of the entire cybersecurity PPP environment by connecting existing partnerships and better leveraging their work across the full spectrum of goals and objectives necessary to secure cyberspace.

Public-private partnership remains a vital and effective tool for achieving the nation's cybersecurity goals. However, the proliferation and evolution of cyber threats continues to outpace efforts to prevent, protect against, mitigate and recover from such attacks, making it evident that more must be done to secure cyberspace. In particular, resources must be focused on research and development, technical standard setting, national and international policy development, and the building of human capital if the U.S. is to shift the balance in its favor.

The creation of dual civic switchboards – complemented with regulatory enhancements where possible – would build upon the accomplishments of existing cybersecurity PPPs, enhancing the efficacy of their work and ensuring that meaningful progress is made across the full spectrum of goals and objectives necessary to secure cyberspace. If implemented in the manner suggested, the recommended alternative will improve the "status quo" of cybersecurity PPPs such that the U.S. is in a position to finally turn the tide on the perpetrators of cyber attacks.

WORKS CONSULTED

Lewis, James A, "Significant Cyber Incidents Since 2006" *Center for International & Strategic Studies,* (2012, January 19), Last Accessed: August 19, 2013, http://csis.org/files/publication/120504_Significant_Cyber_Incidents_Since_2006.pdf.

Frederiksen, N., Lenart, S., "2011 State of Online and Mobile Banking," ComScore Financial Services, Reston, VA: February 2012.

H.R. 3523, 112th Cong., 1st Sess. (2011).

Department of Defense Cyber Crime Center, "Welcome to DC3," Last accessed: August 19, 2013, http://www.dc3.mil/.

Department of Homeland Security, *DHS Risk Lexicon,* (Washington, DC: GPO September 2008).

Department of Homeland Security, Critical Infrastructure, November 30 2010 http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

Gates, R., Napolitano, J., *Memorandum of Understanding between the Department of Homeland Security and the Department of Defense Regarding Cybersecurity,* (Washington, DC: GPO, September 27 2011).

Goldsmith, S, *The Twenty-First Century City: Resurrecting Urban America*. Lanham, MD: Rowman & Littlefield Publishers, Inc, (1999).

International Telecommunications Union, "Global numbers of Internet users, total and per 100 inhabitants, 2001-2011," (2011), Last Accessed: August 19, 2013, http://www.itu.int/ITU-D/ict/statistics/.

National Coordinating Center for Telecommunications, "Program Information." (2011), http://www.ncs.gov/ncc/program_info.html.

Networking and Information Technology Research and Development Program, "Toward a Federal Cybersecurity Game-Changing Research Agenda." (2012), Last Accessed: August 19, 2013, http://cybersecurity.nitrd.gov/.