Journal of Strategic Security

Volume 8
Number 5 *Volume 8, No. 3, Fall 2015* Article 9
Supplement: Eleventh Annual IAFIE Conference

Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership

Max Manley
US Air Force, American Military University

Cyberspace's Dynamic Duo: Forging a Cybersecurity Public-Private Partnership

Author Biography

Max Manley graduated from the US Air Force Academy in 2013 with military honors and a Bachelor of Science degree in Legal Studies. Upon graduation, he was selected to attend the Air Force's intelligence officer school at Goodfellow AFB, TX. Manley is preparing to start his capstone course for his Master's program in National Security Studies at American Military University.

Abstract

As of 2015, cyber threats have become more prevalent due to high-profile cases like the Target, JPMorgan Chase & Co., Home Depot, and Sony Entertainment breaches. In order to prevent what former Secretary of Defense Leon Panetta characterized as a "Cyber Pearl Harbor," the US government has to engage the private sector in order to build a solid public-private partnership (PPP) for cybersecurity. For there to be a successful cybersecurity PPP between the US government and the private sector, there must be a PPP founded on a model composed of four essential elements: a high level of trust between the public and private entities that corresponds to a mutual belief in the positive gains of both partners; clear baseline guidance imposed from legislation, which should be reinforced with government training and financial incentives; a bottom-up structural approach for efficient operations that allows for more autonomy at lower levels on local needs and resources; and, gaining influential community involvement in the formation of PPPs from all levels of the participating organizations, as well as civil leadership and the general public.

Introduction

The use of public-private partnerships (PPPs) is quickly expanding around the world; however, PPPs are not revolutionary answers to complex state needs. For example, back in 1825, the US government and private contractors worked together in the design and construction of the Erie Canal. Another notable example in American history was the Transcontinental Railroad completed in 1869. In the twenty-first century, partnerships among the public and private sectors are not just in transportation developments but also in water and wastewater systems, the supply of social services, and building schools.[1] There are numerous benefits to both public and private sectors when they join in a PPP, such as having a project or operation being more cost-effective and also benefiting from increased availability of resources. Those benefits are enticing cities and countries around the world to combine projects and resources for the betterment of society. Arguably, with all the potential areas desperate for cooperation among public and private sectors, there are few areas of society that are currently more in need for a fully functional PPP framework than in the cyber domain.

Unmistakably, the digital world is becoming more prevalent in life around the world. From Estonia to New York City, the world relies daily on the use of the cyber domain. To put it into perspective, in 2014, a study was conducted on how many US consumers banked online. The study revealed the vast majority of US consumers (approximately eighty-two percent) banked online at least once in the month prior.[2] It is without much debate to conclude that number now is even higher because of the rapid rise and incorporation of technology in most people's daily lives. Furthermore, cyberwarfare and associated threats are swiftly evolving. Everything from an individual's online banking wealth to sensitive national security information are potential targets. Unfortunately, the threat will not be receding anytime in the near future, especially with several examples of highly publicized recent vulnerabilities such as the cyberattacks that shocked Target, JPMorgan Chase & Co., Home Depot, and Sony Entertainment.

In the US, after notorious cyber breaches from the early 2000s to the beginning of 2015, the question remains of what key elements of a PPP must be met for government and the private sector to work together most effectively? For there to be a successful cybersecurity PPP between the government and the private sector, there must be a PPP founded on a model composed of four essential elements: the PPP must be built on trust, clear legal guidance, a bottom-up approach for efficient operations, and community involvement within and surrounding both the public and private entities expressed in terms for the betterment of society. The purpose of this research is to devise a model, from the relevant literature, to explain PPPs, and then to use the constructed qualitative model to investigate the potential success of a PPP in regards to

[1] Mary Corrigan, Jack Hambene, William Hudnut III, Rachelle Levitt, John Stainback, Richard Ward, and Nicole Witenstein, "Ten Principles for Successful Public/Private Partnerships," *Urban Land Institute* (2005): i-35, available at: *http://www.uli.org/wp-content/uploads/2005/01/TP_Partnerships.pdf*.

[2] Nielsen Company, "The Evolution of Modern Banking," *Nielsen Company*, March 19, 2014, available at: *http://www.nielsen.com/us/en/insights/news/2014/the-evolution-of-modern-banking.html*.

the cyber realm. The data used within the devised model originated from secondary raw data already collected from previous studies, surveys, interviews, and research conducted in the field of cyberspace.

General Public-Private Partnership Literature

PPPs in general have been steadily rising around the world. The potential benefits for constructing a PPP include conducting business in a manner that is more efficient and effective. Along with the growth of PPPs, there have been various studies conducted to examine the most advantageous all-purpose criteria for achieving a cooperative PPP.

Osborne structured his book around the fact that since the early 1990s, PPPs have been a "key tool of public policy across the world."[3] PPPs have had successes and failures, but they continue to be perceived by corporations and policymakers as cost-efficient and effective instruments for reaching certain government and private sector agendas. Osborne concluded that the result of a PPP being constructed on a solid framework of pre-determined factors would result in the increased likelihood of prosperity among the public and private businesses.[4]

The end state of a PPP is to "release synergy through collaboration and joining various types of resources, or to transform one or more of the partner organizations."[5] To achieve this, Osborne claimed, most importantly, that there must be a high degree of trust between the public and private entities that corresponds to a "mutual belief in the positive gains of both partners," to the point of almost being like a marriage between two people.[6]

Besides emphasizing the necessary level of trust, Osborne also spent an abundance of time explaining the importance of devising a bottom-up approach to the overall operational structure between the public and private organizations. In the past, a more "rigid set of formal partnerships" based on strict "legally binding contract(s)" were utilized to form PPPs.[7] These rigid forms of PPPs eventually discouraged teamwork and efficiency since the majority of operations were directed from a top-down hierarchy. Osborne warned that this could lead to a reduction in voluntary cooperation from both sides. Further, if both sides of the partnership are weary of strict constraints enforced from a distant command structure, then the PPP will not be able to respond to the fluid nature of threats such as a cyberattack.[8]

The difference between implementing a top-down versus a bottom-up style of operational structure is that the top-down involves a more concentrated flow of authority, like an agency of the central government enacting specific guidance and

[3] Osborne, Stephen, *Public-Private Partnerships* (London: Public-Private Partnerships, 2005), available at: *http://samples.sainsburysebooks.co.uk/9781134615063_sample_517085.pdf*.
[4] Ibid.
[5] Ibid, 14.
[6] Ibid.
[7] Ibid, 16.
[8] Ibid.

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478

pushing that guidance down the chain of command. On the other hand, the bottom-up approach allows for more autonomy at lower levels on local needs and allocation of resources to accomplish the objectives. Osborne used an example implemented in the UK's distribution of government funds. The example described how the UK's central government allocates funds to several local community workers to work on building projects in order for communities at the lower levels to initiate their own directives for intended projects.[9] Osborne's research highlighted critical components to reference when creating successful PPPs. Two critical components were building trust and a fluid bottom-up approach.

In Zhang's article, the author identified unique criteria for general PPPs. In his analysis, Zhang reviewed what the World Bank had previously recorded as contributing factors to failed PPPs around the world. Some of the World Bank's most common reasons for why several PPPs had failed throughout the international community were: (1) "Wide gaps between public and private sector expectations;" (2) "lack of clear government objectives and commitment;" (3) "complex decision making; inadequate legal/regulatory frameworks;" (4) "poor risk management;" (5) "low credibility of government policies;" and (6) "poor transparency."[10] After narrowing the issue, Zhang performed an extensive literature review, case studies, and interviews with world-wide PPP experts to devise his five essential factors for implementing a successful PPP. For purposes of this paper, only three of the five are relevant to the construction of a PPP related to cyberspace in the US. Those relevant were the (1) "economic viability;" (2) "appropriate risk allocation via reliable contractual arrangements;" and (3) having a "sound financial package."[11] All of these criteria can reasonably relate back to having a clear objective and guidance for the PPP, usually from some form of contract or legislation action.

Zhang further emphasized the critical nature for PPPs with transparency, flexibility, and particular public funding incentives. Reasonably, government and private joint ventures would benefit from having "established common objectives and defined procedures for collaborative problem solving"[12]; however, to obtain this there must be some of the detailed factors Zhang expressed. Zhang came across something universal in his interviews, which was how corruption typically set in for partnerships. Often times, corruption in partnerships arose from a lack of transparency and loss of interest.[13] To alleviate the potential for this to occur, Zhang recommended that PPPs shift from a traditional regulatory stance to a more "liberal and dynamic outlook," similar to a bottom-up approach for operational structure.[14] Additionally, Zhang proposed that there should be incentives on behalf of the public enterprise, in the form of government subsidies, to encourage a stronger relationship and dialogue with the private sector.[15] Zhang's article dealt mostly with financial businesses working towards urban

[9] Ibid.
[10] Xueqing Zhang, "Critical Success Factors for Public-Private Partnerships in Infrastructure Development," *Journal of Construction Engineering & Management* 1:131 (2005): 3-14.
[11] Ibid, 13.
[12] Ibid, 4.
[13] Ibid.
[14] Ibid, 7.
[15] Ibid.

development projects in regards to PPPs; however, the financial aspects and clear government guidance addressed in Zhang's article could realistically be applied for any form of future PPPs.

Cheung, Chan, and Kajewksi wrote a collaborative academic paper recording results of questionnaire surveys meant to elicit responses from businesses in Hong Kong and Australia. In the survey, which received thirty-four completed questionnaires from Hong Kong and eleven from Australia, the participants were asked to rate eighteen factors in order of importance in regards to establishing a productive PPP. After the results were gathered, Cheung, Chan, and Kajewski compared the findings to results in a similar survey conducted in the UK. The findings revealed three common responses for all three countries represented. Those factors were: (1) "Commitment and responsibility of public and private sectors;" (2) "strong…private consortium;" and (3) "appropriate risk allocation and risk sharing."[16] These results demonstrated that there are common threads across the world's PPPs that are considered significant factors towards cooperation and successful partnerships. The top three responses are practically associated to a sharing of commitment and responsibility among the partners that originates from having established a trusted relationship.

Another key aspect that Cheung, Chan, and Kajewski mentioned for a PPP was the necessity among partners for an "independent, fair and efficient legal framework."[17] This conclusion in the article was derived from the 2007 National Treasury PPP Unit of South Africa, which shined a light on the importance of how legal guidelines are drafted, especially with the government being able to provide sufficient legal resources at reasonable costs to deal with the majority of the legal process. In the end, the goal of the legal framework is to have a PPP where public and private sectors "bring their complementary skills and commit their best resources to achieve a good relationship."[18] In the US, for national level agreements, the initiation of the legal framework would reside with the two houses of Congress and the Office of the President.

Finally, Trafford and Proctor conducted a survey of thirty subjects pooled from senior managers, middle managers, and lower-positioned staff employed by city councils, the private sector, and joint venture companies. Trafford and Proctor solicited those individuals for being "instrumental" in the establishment of joint ventures, such as PPPs.[19] In essence, the community within and surrounding both the public and private entities were researched in how they contributed to the various organizations in successfully executing PPPs.

In one example, Trafford and Proctor referenced conclusions made by former UK Prime Minister Tony Blair in 1998. Blair claimed, "The days of all-purpose authority that plans

[16] Esther Cheung, Albert P.C. Chan, and Stephen Kajewski, "Factors Contributing to Successful Public Private Partnership Projects," *Journal of Facilities Management* 10:1 (2012): 45-58.
[17] Ibid, 53.
[18] Ibid, 54.
[19] Sue Trafford and Tony Proctor, "Successful Joint Venture Partnerships: Public-Private Partnerships," *The International Journal of Public Sector Management* 19:2 (2006): 117-129.

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478

and delivers everything are gone…partnership with others— public agencies, private companies, community groups and voluntary organizations" is where the social structure is heading.[20] Furthermore, public support campaigns can potentially rally behind and encourage the creation of PPPs. As more pressure, from political leadership to the general public, is applied to the potential PPPs, then the probability of a partnership is likely to increase. In other words, PPPs can be constructed when there is an important issue at stake for the leader of a nation or the public at large, and thus the public and its representatives can persuade public and private sector entities to eventually join into partnerships.

Gathered from the relevant literature already written on constructing a successful PPP, there were four essential elements extracted that were deemed necessary when applying a model for US PPP to address the issue of cybersecurity. Osborne demonstrated that there requires a high-level of trust to be established between parties in a PPP.[21] Additionally, Osborne detailed how a bottom-up approach to a PPP's organizational structure is advantageous for flexibility and efficiency in responding to issues. While Osborne covered the relationship and authority that needs to be developed among parties of a PPP, Zhang focused on the monetary requirements or incentives that are crucial for a PPP to be successful.[22] Also, Cheung, Chan, and Kajewski covered the important criteria of a strong, clear legal framework, as well as explaining the necessity of sharing inherent responsibilities of the commitment.[23] Lastly, from the literature reviewed, Trafford and Proctor illustrated the importance of gaining cooperation in the formation of PPPs from various levels of the proposed partnership community.[24] Trafford and Proctor also recalled the influence of civil leadership in the formation of PPPs.

Cybersecurity Public-Private Partnership Model

The variables analyzed from the applicable literature can be closely related together for the purpose of creating a model. The model methodology can be used for doing predictive analysis, especially when attempting to investigate how the public and private sectors should join together in a PPP with the intent of strengthening the nation's cybersecurity structure. The data found for use in building the model was a mixture of secondary raw data. The secondary raw data consisted of specific remarks or speeches from influential members in regards to cybersecurity within both the public and private sector, newspaper articles addressing cybersecurity, reports on historical case studies involving previous attempts to form cyber-related PPPs in other countries and global regions, and survey reports conducted with cyber professionals or cyber companies.

[20] Ibid, 119.
[21] Osborne, *Public-Private Partnerships.*
[22] Zhang, "Critical Success Factors for Public-Private Partnerships in Infrastructure Development."
[23] Cheung et al., "Factors Contributing to Successful Public Private Partnership Projects."
[24] Trafford and Proctor, "Successful Joint Venture Partnerships."

The four essential elements built from the theories for successful PPPs from the literature review are incorporated, from bottom to top, in a figure below to help illustrate the model created.

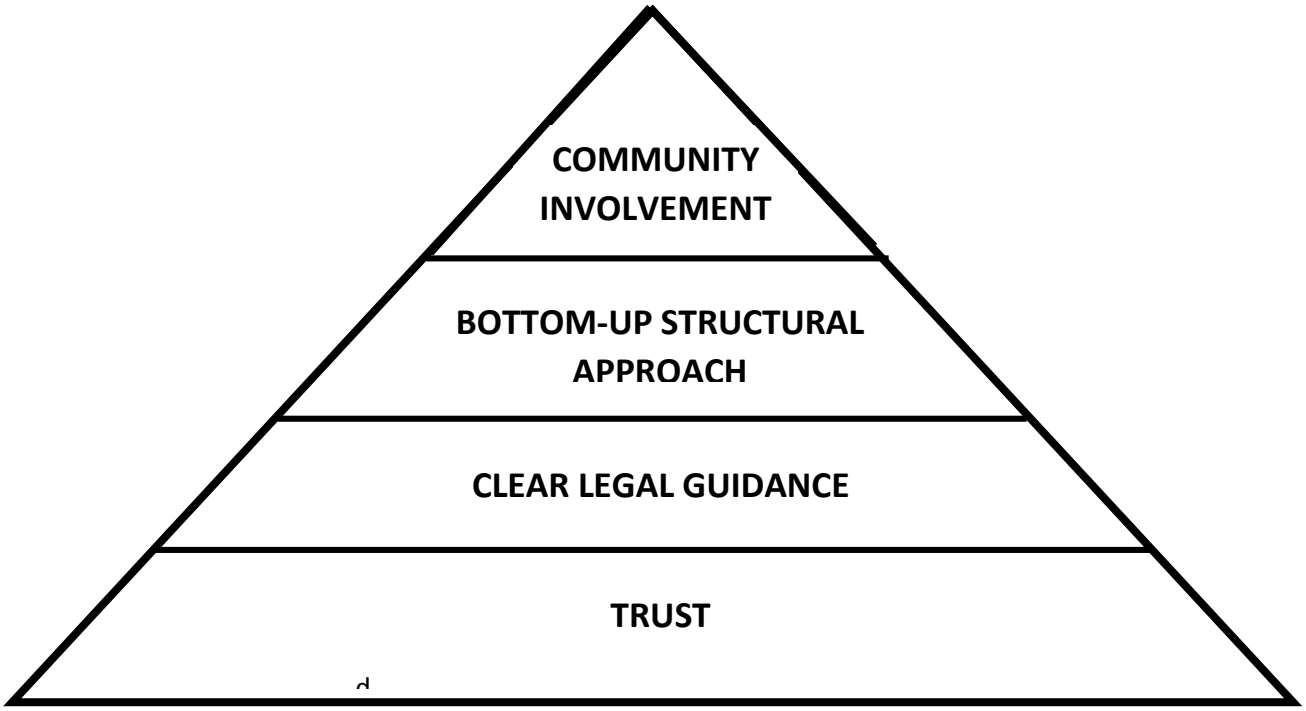

Figure 1. Qualitative Model for Successful Public-Private Partnerships

Step One: Building a High-Level of Trust

The first step to any successful PPP is for all parties to be in an agreement built on a high-level of trust. Nearly every piece of literature studied covering PPPs mentioned the significance of trust within the commitment. There can be substantial rhetoric promoting honesty between the parties involved; however, if there are no signs of trust being built through substantive actions then the flow of any voluntary information not required by the proposed law or contract will cease almost immediately. Building confidence in the private and public entities can be completed through small efforts initially that lead to a successfully shared goal being reached and eventually build up to a trusted relationship.[25] Another way of stating this would be that "success breeds confidence, and confidence breeds trust."[26] Interestingly, studies of business relationships show that all of the PPP's communication does not necessarily always have to be formal dialogues; informal styles of communication, such as merely emailing a colleague who works at a different agency within the PPP to ask for an update on his or her work and family, could also be employed to build the trusted relationship.[27] Personal relationships could be built through the communication channels established

[25] Corrigan et al., "Ten Principles for Successful Public/Private Partnerships."
[26] Ibid, 30.
[27] Osborne, *Public-Private Partnerships*.

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478

via the PPP, such as secured network chatrooms or emails. Once those relationships continue to build upon the shared cybersecurity goals being pursued, then the PPP will further increase in productivity.

Understandably, if private companies cannot trust the government with their information, why participate in a PPP with the government? Presently, the private sector is extremely reluctant on sharing information with the US government detailing sensitive information about customers or consumers using their products or services. Furthermore, companies are even hesitant to share information about disastrous cyberattacks or breaches of information with the US government, even though the government could provide tools to track down the hackers.[28] Former Director of the National Security Agency, Keith Alexander, noted that the complex problems posed by cyberattacks do not require sacrificing civil liberties for security.[29] Public statements like the one Director Alexander made is a step in the right direction for building a trusted relationship, but living up to that promise through observable actions will inevitably build greater "trust and strict confidentiality" for future members of cyber-orientated PPPs.[30]

A case study released in a 2014 report analyzed a PPP with regards to cyber entities within the Netherlands. In the Dutch example, early on in the PPP, privacy concerns were raised. Several companies feared, as many US companies have, that willingly allowing the government access to their networks might put their data or their customers' data at risk.[31] The companies in the Netherlands went so far as to claim that even the publicity that the government had access to customer's accounts would cause a loss in business.[32] The only way to overcome this fear is to have a solid relationship founded on trust and transparency. Of course, a realistic PPP will never be completely transparent, but if the foundation of trust had been properly laid then there is a greater chance for the relationship to remain strong. The privacy solution that the Netherlands's government implemented in its PPP with Dutch companies was to have a network system designed that prevented direct access to any consumer information without the companies' consent and manual intervention.[33] If the US government is able to provide this same level of confidence to the American private sector, then there is a better possibility that the PPP will be successful.

An example in January 2015 of where the government failed to develop a relationship of trust with its private companies is that of newly proposed laws in Thailand. Reportedly, Thailand's military-appointed legislature proposed a bill that would allow for mass

[28] Emily Goldman and John Arquilla, "Cyber Analogies," Naval Postgraduate School (November 28, 2014): 1, available at: *http://calhoun.nps.edu/bitstream/handle/10945/40037/NPS-DA-14-001.pdf?sequence=1*.
[29] Corey Gray, "Cyber Utilities Infrastructure and Government Contracting," *University of Miami National Security and Armed Law Review* 8:1 (2013), 151-171.
[30] Ibid, 162.
[31] Kas Clark, Don Stikvoort, Eelco Stofbergen, and Elly van den Heuvel, "A Dutch Approach to Cybersecurity," *IEEE Computer and Reliability Societies* (September/October, 2014): 27-34.
[32] Ibid.
[33] Ibid.

persistent government surveillance of citizens' online activities and platforms.[34] The specifics of the bill would allow a government-run cybersecurity committee the authorization to access information on personal computers, cell phones, and other electronic devices without a court order if deemed necessary by the government for "national security."[35] To place into context for the future cyber-related PPPs in the US, if the US government was to completely circumvent the judicial system as Thailand is proposing, then there would be a public relations disaster erasing any chance for future trust to be built.

Privacy and the prerequisite of reliable trust is undoubtedly on the minds of the Chief Executive Officers (CEOs) of major companies across the US. For example, at the White House Summit on Cybersecurity and Consumer Protection in February 2015 at Stanford University, Apple's CEO Tim Cook stated, "If those of us in positions of responsibility fail to do everything in our power to protect the right of privacy, we risk something far more valuable than money…We risk our way of life."[36] At the conference, the federal government was hoping for more dialogue on how to create an effective PPP in the near future; however, throughout the conference, the dialogue consisted of multiple CEOs strongly requesting the government to share more information about threats or classified intelligence that could prevent a future breach.[37] There is a desire for a quid pro quo between the private companies and the US government; however, it appears that the CEOs perceive the future PPP as more of a benefit for the government to gain access to its information without a reciprocal value of receiving government information that could possibly spoil an attack. As of the end of February 2015, major private companies present the impression that if any PPP is further pressured onto them, it will not be well received since there is already a sense of distrust established between the parties. The first level of the pyramid model for an effective PPP within the cyber domain is not completely satisfied at the present point in 2015.

Step Two: Creating Clear Legal Guidance

While the first level of the model regards building a sense of trust among the parties within a PPP, the next step focuses on establishing clear baseline legal guidance to nurture a trusted relationship. PPPs can be formed two different ways, which are collaborative (non-legally binding) or contractual (legally binding) agreements.[38] Arguably, the most conducive partnership for teamwork and communication is a bottom-up approach built by a collaborative partnership; however, while collaborative partnerships can promote "goodwill gestures…and provide knowledge exchange or

[34] "Cyber Security Bill Threatens Media Freedom in Thailand," Committee to Protect Journalists, January 20, 2015, available at: *https://cpj.org/2015/01/cyber-security-bill-threatens-media-freedom-in-tha.php*.
[35] Ibid.
[36] Danny Yadron and Damian Paletta, "Cybersecurity Summit exposes Concerns about Privacy," *Wall Street Journal*, Feb 13, 2015, available at: *www.wsj.com/articles/cybersecurity-sumit-exposes-silicon-valleys-privacy-fears-1423862917*.
[37] Ibid.
[38] Pat Cummens, Rick Webb, Angela Firkins, Doug Robinson, and Stephanic Czwhajewski, "Keys to Collaboration: Building Effective Public - Private Partnerships," *Contract Management* 9 (May 2006).

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478

collectively leverage resources for a specified goal," they are not binding.[39] Therefore when predicting the proper form of a PPP between the US government and the private sector, the required legal framework will be legislation signed by the President, which is contractual rather than simply collaborative.

Whatever PPP is built between public and private cyber entities, it will have to fall under the supreme law of the land, the Constitution of the United States. The Fourth Amendment to the Constitution affords US citizens all the right to "be secure in their persons, houses, papers, and effects, against unreasonable search and seizures."[40] The legislation or contract enacted will have to be governed ultimately by the protection afforded from the Fourth Amendment and thus establish a baseline level of security for private companies. Moreover, this will lend to a standard of trust being established.

As suggested earlier, Congress and the Office of the President will most likely be involved in establishing any sort of cybersecurity PPP. Congress has consistently failed to pass legislation to protect the national-level cyber systems.[41] Specifically, in 2012, a Senate bill pertaining to cybersecurity never made it out of committee because it failed to define how the PPP would "maintain civil liberties and [ensure] public safety."[42] While throughout most of the twenty-first century Congress and the President have been behind the learning curve when it came to legislation in cybersecurity, in 2014 there was the passage of the National Cybersecurity Protection Act and the Federal Information Security Modernization Act of 2014.[43] Both of those pieces of legislation were progressive actions; however, there should be revised legislation that promotes more autonomy at the lower levels and provides clear guidance of standard baseline cybersecurity practices. Furthermore, the US government is still behind in eliciting confidence from the private sector, even with the aforementioned pieces of legislation. There will be difficulty in encouraging voluntary sharing of sensitive information until there is an established level of trust and a sense of mutual benefit set by law.

Something additional that the US government could implement legally would be financial incentives for further collaboration with the private sector. Cybersecurity operations and the costs associated to defend in the cyber domain are rather expensive. For example, JPMorgan Chase & Co.'s CEO claimed his company "spends approximately $200 million to protect… from cyberwarfare and to make sure our data are safe and secure [with 600 people dedicated to the task]."[44] When drafting congressional legislation or presidential executive orders, there could be incentives incorporated, such as training opportunities for some of the cybersecurity departments within influential private sector companies like JPMorgan Chase & Co. The US government has the ability

[39] Ibid, 4.
[40] U.S. Constitution, amend IV.
[41] Gray, "Cyber Utilities Infrastructure and Government Contracting."
[42] Ibid, 159.
[43] John Lainhart and Dan Chenok, "Legislation and the Future of Federal Cybersecurity," *Business of Federal Technology*, February 18, 2015, available at: *http://fcw.com/articles/2015/02/18/legislation-and-cybersecurity.aspx*.
[44] Libicki, Martin, David Senty, and Julia Pollack, *Hackers Wanted: An Examination of the Cybersecurity Labor Market* (Washington: RAND, 2014).

to pass along some training and resources, and in return the private companies will likely be more open to sharing information and consider the PPP more as a collaboration than a stipulation. As of 2015, Congress and the President are attempting to change the course the US has been heading in regards to national cybersecurity; particularly, the legislative acts that were able to pass Congress in 2014 are slowly being implemented and are providing opportunity for there to be an even closer PPP between the US and private companies. In accordance with the model proposed in this paper, the US is now formulating a clearer source of legislative direction; the key to success of the forthcoming PPP is what form of relationships will government organizations take in executing the legislation. If it is perceived as being forced upon the companies, there is the probable risk for US companies to combat the mandates in creative ways like using various encryptions and limiting voluntarily shared information to elude government oversight and loss of privacy to itself and its customers.

Step Three: Implementing a Bottom-up Organizational Structure

For when applying a clear legal guidance, the next layer in the model for an effective PPP is establishing a bottom-up approach for the organizational structure of the PPP. The PPP authority cannot be dictated solely by one central government entity, like the Department of Homeland Security or US Cyber Command. For example, Australia and Great Britain have in place strict "draconian measures" in their PPPs with private companies for how those companies are to invest in cyber defense and share internal data about attacks.[45] The level of sharing is reportedly limited due to the established top-down approach to the relationship.

On the other hand, there is the successful example of a cybersecurity PPP in the Netherlands. In the Dutch collaboration, the National Cybersecurity Center (NCSC-NL) actively encourages participation from the private companies via conferences held where public and private organizations physically sit down together and discuss all the terms and conditions for how the network sharing is constructed.[46]

In obtaining a successful cybersecurity PPP in the Netherlands, the process built upon lessons learned from failed earlier attempts. Back in the early 2000s, the government ran a PPP similar to that of the UK and Australia's current PPPs, where it was a top-down authoritative structure. Don Stikvoort, who ran the Netherlands's government cybersecurity organization in the early stages, specified after the first PPP failed, "When partners feel that they're equals, they're more willing to participate than when they feel that one partner holds more power than the others. When one partner begins making demands, voluntary collaboration stops."[47] Stikvoort presided over a PPP that ultimately failed in two years and was eventually reconstructed into the current successful PPP in the Netherlands. The current bottom-up approach moves past "strict, hierarchical models" and represents where "all partners have an equal seat at the table."[48]

[45] Gray, "Cyber Utilities Infrastructure and Government Contracting."
[46] Clark, Stikvoort, Stofbergen, and Heuvel, "A Dutch Approach to Cybersecurity," 32.
[47] Ibid, 28.
[48] Ibid, 33.

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478

The US government should take notice of the Dutch government's initial failures. When the Netherlands demanded specific cooperation, the private companies pushed back with devising new ways of operating to evade government interaction. Now, the Dutch government and private companies work on a secure network equally and consistently sharing information across several levels and chains of command for fast responses to cyber threats.[49] Of course there should still be clear lines of authority in times of national crises or emergencies; however, if the US government initiates a PPP where the private industry is equally considered in discussions, then the relationship will likely harvest more sharing then if a top-down approach is used as the sole structure of operation.

Similar collaboration platforms to the Dutch example also exist in other regions of the world. For example, in the Asia-Pacific region, Asia-Pacific Computer Emergency Response Team (APCERT) coordinates the entire Asia-Pacific region's incident responses by developing trusted relationships among national-level entities.[50] APCERT is a group of over thirty emergency response teams spanning several countries across the Asia-Pacific region to deal with "large-scale or regional network security incidents, facilitate information sharing and technology exchange, and promote collaborative research and development."[51] Interestingly enough, this collaboration even includes political adversaries, such as China and Taiwan.[52] If China and Taiwan are able to share even the slightest amount of cybersecurity information, it is within reason for the US government and private corporations to join in a PPP where information flows more freely.

Furthermore, the significance of having a bottom-up approach allows for a faster response at the lower levels in addressing potential cyber threats. If the PPP has a bottom-up approach, then those parties at the lower levels will have more autonomy to react quicker to cyberattacks, thus being more resilient over time. An example of this concept in action is the report of a joint venture by the Rockefeller Foundation's "100 Resilient Cities" and Microsoft to provide cybersecurity expertise training and funding at local city levels across the world. The intent behind the "100 Resilient Cities" initiative is to give those entities at the bottom sufficient training and resources to act alone and become "more resilient to the shocks and stresses" that are a growing part of cyberspace.[53] This is yet another example of how the US government can provide the training, education, and resources to allow private companies the ability to be more independent and resilient. As a result, the government training and support can provide

---

[49] Clark, Stikvoort, Stofbergen, and Heuvel, "A Dutch Approach to Cybersecurity."
[50] Ibid.
[51] Catriona Heinl, "Regional Cyber Security: Moving Towards a Resilent ASEAN Cyber Security Regime," Rajaratham School of International Studies (2013): 35, available at: *http://dr.ntu.edu.sg/rsis/publications/WorkingPapers/WP263.pdf*.
[52] Clark, Stikvoort, Stofbergen, and Heuvel, "A Dutch Approach to Cybersecurity."
[53] "100 Resilient Cities and Microsoft Announce Partnership to Help Cities Build Cybersecurity," 100 Resilient Cities, January 15, 2015, available at: *http://www.100resilientcities.org/blog/entry/100-resilient-cities-and-microsoft-announce-partnership-to-help-cities-buil#/-_/*.

improved stability across the country at lower-levels in response to cyberattacks and breaches.

Step Four: Involving the Community

The final level, the highest point of the model depicted in figure one, is the influence of the community involved, both within the organizations and outside, in rallying support for the parties to enter a PPP; in other words, is the PPP worth entering for both parties and the community it represents? According to a RAND Corporation report, the US government and its civil leadership paid little attention to the threats posed by cyberattacks prior to 2007.[54] The change of focus likely arose after the massive cyberattacks on Estonia and documentation about Chinese intrusions in the Department of Defense in 2007.[55] In fact, the report claimed the first official government recognition of the significance of cybersecurity in the public and private sectors was the 2008 Comprehensive National Cybersecurity Initiative.[56]

Now, in 2015, both the public and private sectors actively advocate for greater cybersecurity enterprises, particularly sharing of vital cyber threat information without loss of privacy. Realistically, the US is still relatively vulnerable in several aspects of its critical infrastructure. One analyst illustrates the catastrophe that could unfold if there is not a successful PPP by describing "an attack on the US will… be with [an] anonymous click of a mouse that turns off power grids, releases flood waters of dams, and melts down nuclear reactors.[57]

In regards to the utilities infrastructure of the US, the Department of Energy (DOE) has proactively requested for Congress to "[facilitate] public-private partnerships to accelerate cybersecurity efforts for the twenty-first century; fund research and development of advanced technology to create a secure and resilient electricity infrastructure; [and] support the development of cybersecurity standards to provide a baseline to protect against known vulnerabilities."[58] The DOE has numerous threats to potentially prepare against, and utilizing a future established line of communication via a PPP with the private sector cyber community will provide the DOE with the ability to react faster and with greater precision to posed threats.

Over the past few years, strategic rhetoric from prominent political leaders has risen in regards to the need to defend the country's cybersecurity. Former Secretary of Defense Leon Panetta on October 11, 2012, warned that the US is vulnerable to a "Cyber Pearl Harbor."[59] Furthermore, President Obama articulated on December 19, 2014 after the Sony Entertainment breaches:

---

[54] Libicki, *Hackers Wanted*.
[55] Ibid
[56] Ibid
[57] Gray, "Cyber Utilities Infrastructure and Government Contracting," 171.
[58] August Roesener, Carl Bottolfson, and Gerry Fernandez, "Policy for US Cybersecurity," *Air & Space Power Journal* 28:6 (Nov 2014): 32.
[59] Goldman and Arquilla, "Cyber Analogies," 26

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478

> "This is part of the reason why it's going to be so important for Congress to work with us and get an actual bill passed that allows for the kind of information-sharing we need. Because if we don't put in place the kind of architecture that can prevent these attacks from taking place, this is not just going to be affecting movies, this is going to be affecting our entire economy in ways that are extraordinarily significant."[60]

As evident by all the senior US officials or former senior US officials' rhetoric, the leadership of the US government has set the tone for cyberattacks and breaches as a very serious issue that needs more collaboration with the private sector.

While the public sector is vocally and legislatively becoming more insistent on PPPs in regards to cybersecurity, voices within the private sector are still hesitant to fully commit publically to a PPP. The reluctance to join in a PPP could likely be credited to the potential for the government to gather mass amounts of sensitive information on company and customer information; however, there still remains hope for a stronger PPP to be constructed based on evolving opinions. Apple CEO Tim Cook proclaimed the following at the 2015 White House Summit on Cybersecurity: "Security and convenience can work in harmony…. No single company or organization can accomplish this on its own. We are committed to engaging with the White House and Congress and putting things into action."[61] Additionally, MasterCard CEO Ajay Banga acknowledged President Obama and Congress' efforts to legislatively address cybersecurity concerns, but also warned, "We need a real legislative solution….Rather than fight this in individualized groups, there's some merit in joining hands and doing it together."[62] While these comments represent only two prominent members of the private sector, they do have significant corporate influence in setting the tone on how companies accept new congressional and executive measures that are enacted. The remarks are optimistic, but concerns about privacy rights and the government's ability to seize certain sensitive information of companies or customers are still ubiquitous.

Conclusion

While PPPs are becoming more predominant around the world, the concept is not unique to recent years; however, the precise process of implementing a PPP is distinctive and particularly important. Throughout history, there have been numerous examples of successful and failed attempts at creating a PPP. As discovered from the literature, if there is to be a successful PPP between the government and the private

---

[60] Securing Cyberspace - President Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Washington, D.C.: White House, 2015), available at: *http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat*.

[61] Julie Clover, "Apple CEO Tim Cook Speaks at White House Cybersecurity Summit," *MacRumors*, February 13, 2015, available at*: http://www.macrumors.com/2015/02/13/apple-ceo-tim-cook-cybersecurity-summit/*.

[62] Katie Zezima, "Obama Signs Executive Order on Sharing Cybersecurity Threat Information," *Washington Post*, February 12, 2015, available at: *http://www.washingtonpost.com/blogs/post-politics/wp/2015/02/12/obama-to-sign-executive-order-on-cybersecurity-threats/*.

sector that operates within cyberspace, there must be a PPP founded on four essential elements: trust, clear guidance based upon contracts or some other legal enactment, a bottom-up approach for operational structure, and community involvement within and surrounding both the public and private entities.

From reviewing surveys, interviews, case studies, speeches and reports conducted from prominent cyber professionals in both the public and private sectors, the US is headed in an encouraging direction for implementing a successful PPP. There still needs to be a greater extent of trust formulated, but that will take time. Nevertheless, as soon as the US government begins dictating how and when companies operate in regards to the cyber domain without allowing for an open dialogue on equal standing, then the communication between the parties will weaken and the PPP will ultimately fail, as it had previously for other countries like the Netherlands. The President said it best himself, in regards to where the US needs to head in a cyber PPP: "There's only one way to defend America from these cyber threats, and that is through government and industry working together, sharing appropriate information as *true partners*" (emphasis added).[63]

[63] Ibid.

https://scholarcommons.usf.edu/jss/vol8/iss5/9
DOI: http://dx.doi.org/10.5038/1944-0472.8.3S.1478