2015

Using the Oldest Military Force for the Newest National Defense

Brian Claus

Robin A. Gandhi

Julia Rawnsley

John Crowe

Journal of Strategic Security

Volume 8
Number 4 *Volume 8, No. 4: Winter 2015*

Article 1

Using the Oldest Military Force for the Newest National Defense

Brian Claus
United States Strategic Command, CLAUSB@stratcom.mil

Robin A. Gandhi
The University of Nebraska at Omaha, rgandhi@unomaha.edu

Julia Rawnsley
The University of Nebraska at Omaha, jrawnsley@unomaha.edu

John Crowe
The University of Nebraska at Omaha, johncrowe@unomaha.edu

pp. 1-22

Recommended Citation
Claus, Brian; Gandhi, Robin A.; Rawnsley, Julia; and Crowe, John. "Using the Oldest Military Force for the Newest National Defense." *Journal of Strategic Security* 8, no. 4 (2015): : 1-22.
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441
Available at: http://scholarcommons.usf.edu/jss/vol8/iss4/1

Using the Oldest Military Force for the Newest National Defense

Author Biography

Mr. Brian Claus is a Targeting Officer for United States Strategic Command (USSTRATCOM) at Offutt Air Force Base, Nebraska and a squadron commander in the Iowa Air National Guard. He is also a 2015 USSTRATCOM Strategic Leadership Fellow at University of Nebraska Omaha where he performed research in critical infrastructure cyber defense. He received his Master's Degree in Aerospace Studies from Embry Riddle Aeronautical University and Bachelor of Science in Computer Science from South Dakota State University.

Dr. Gandhi is an Associate Professor of Information Assurance at the University of Nebraska at Omaha. He received his Ph.D. from The University of North Carolina at Charlotte. His research, teaching, and publications are in the areas of information assurance, regulatory requirements modeling and analysis, software assurance, certification and accreditation and risk assessment. AFOSR, NIST, NASA, NSF, DHS S&T and AFRL have supported his research. He is a member of IEEE and ACM professional communities and the DHS Software Assurance Workforce Education and Training Group.

John Crowe is a Navy veteran who is in his third year as a doctoral student in Industrial and Organizational Psychology at the University of Nebraska at Omaha. He holds a bachelor's degree in Psychology, with a minor in Sociology, from Creighton University. In his time at UNO, John has worked on several projects applying principles of organizational science, collaboration, and leadership to the study of both conventional and non-conventional organizations. John has assisted on the United States Strategic Command Leadership Fellows Program in which he helped develop an experiential leadership program for high performing STRATCOM civilian employees. John has presented his research at several national and international conferences, including the International Studies Association, the American Psychological Association, Interdisciplinary Network for Group Research, and the Society of Industrial and Organizational Psychology.

Julia Rawnsley is a graduate student at the University of Nebraska at Omaha in the Master's of Business Administration program, where she also received her bachelor's degree. Her research interests include environmental sustainability and the industry of death care.

Abstract

The National Guard is establishing Cyber Mission Teams (CMT) that will fulfill a federal role to backfill active duty defending Department of Defense networks, but are also exploring how they could effectively fulfill state missions. The President, Council of Governors, and USCYBERCOM Commander have expressed concerns about U.S. critical infrastructure cyber network vulnerabilities and the increasing magnitude of threat our adversaries pose to those networks' security. This article explores using this emerging National Guard capability

in a state role for protection of critical infrastructure cyber networks. Most of the critical infrastructure is privately owned. Although current executive orders and policy mandate government sharing of cyber threat information, private providers' reciprocation of sharing their vulnerabilities is voluntary. This article contends that effective cyber defense requires strong private-public partnerships. We developed a critical infrastructure cyber defense model based upon key characteristics from the literature on private-public partnerships and performed a case study of current cyber defense partnerships to validate the model. Our research shows this model to be a useful guide for emerging National Guard Cyber Mission Forces to consider when establishing partnerships for effective critical infrastructure cyber defense.

Introduction

Approximately 85 percent of America's critical infrastructure is owned and operated by private industry.[1] According to the National Institute of Standards and Technology (NIST), the daily operations of our nation's critical infrastructure are controlled by Industrial Control Systems (ICS). Initially, ICS had little resemblance to traditional information technology systems in that ICS were isolated systems running proprietary control protocols using specialized hardware and software. Remote maintenance access to ICS systems is more prevalent now since low-cost Internet Protocol devices are widely available. This has made ICS systems more susceptible to outside threats.[2] In 2014, over 52,000 cyber security incidents occurred on some form of critical infrastructure network.[3]

Attacks in the past ten years have shown that an attack from cyberspace could seriously damage or disrupt our energy infrastructure. In January 2014, Colorado Governor John Hickenlooper, the vice chair of the National Governors Association, warned his fellow governors that, "the next battlefront is likely not a field or town, but a computer network that supports our critical infrastructure."[4] According to Admiral Michael Rogers, the USCYBERCOM commander, in his March 4, 2015 testimony before the House Armed Services Committee, "The U.S. government, the states and the private sector can't defend their information systems on their own against the most powerful cyber forces." He also commented that, "We believe potential adversaries might be leaving cyber fingerprints on our critical infrastructure, partly to convey a message that our homeland is at risk if tensions ever escalate toward military conflict."[5] The costs to harden the US energy sector against cyber-attacks are projected to be more than $7 billion by 2020 for the electric power industry and nearly $2 billion by 2018 for the oil and gas industry. Now,

---

[1] Nathan E. Busch, and Austen D. Givens, "Public-Private Partnerships in Homeland Security Opportunities and Challenges," *Homeland Security Affairs* 8 (October 2012).
[2] Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to Industrial Control Systems (ICS) Security," NIST Special Publication (2011): 800-82.
[3] Verizon Corporation, "2015 Data Breach Investigations Report," *Verizon*, 2015, available at: *http://www.verizonenterprise.com/DBIR/2015/*
[4] William Matthews, "Cyber Uncertainty," National Guard: The Official Publication of the National Guard Association of the United States, July 2014, available at: *http://nationalguardmagazine.com/display_article.php?id=1764536&id_issue=218066*
[5] Cheryl Pellerin, "CYBERCOM Chief: Cyber Threats Blur Roles, Relationships," *Official Wire*, March 6, 2015, available at: *http://www.officialwire.com/news/cybercom-chief-cyber-threats-blur-roles-relationships/*

more than ever, there is a higher need for more efficient critical infrastructure cyber defense.[6]

Federal Role in Homeland Cyber Defense

Executive Order 13636 mandates the Secretary of Homeland Security in collaboration with the Secretary of Defense will provide classified cyber threat and technical information to eligible private critical infrastructure companies.[7] While the sharing of that information by private industry is highly encouraged, it is purely voluntary.

One result of this mandate was the establishment of the National Cybersecurity & Communications Integration Center (NCCIC), which serves as a 24/7 centralized location for the coordination and integration of cyber situational awareness and incident management. NCCIC partners include all federal departments and agencies; state, local, tribal, and territorial governments; the private sector; and international entities. The NCCIC provides its partners with enhanced situational awareness of cybersecurity and communications incidents and risks, and provides timely information to manage vulnerabilities, threats, and incidents. In 2014, the NCCIC received over 97,000 incident reports, and issued nearly 12,000 actionable cyber-alerts or warnings. NCCIC teams also detected over 64,000 vulnerabilities on federal and non-federal systems and directly responded to 115 significant cyber incidents.[8] The NCCIC also relies heavily on voluntary collaboration with its partners. The Center provides, free of charge, penetration analysis and vulnerability assessments on cyber networks for critical infrastructure providers in a private-public partnership (PPP).

National Guard Role in Homeland Cyber Defense

In 2013, lawmakers in Congress introduced the Cyber Warrior Act that would create a Guard Cyber and Network Incident Response Team for each state. The teams would leverage private-sector IT experts in the Guard and could be called on by governors and the defense secretary to respond to cyber

---

[6] A. Kambour, *Enhancing the Cybersecurity of Energy Systems and Infrastructure* (Washington, D.C.: National Governors Association Center for Best Practices, August 4, 2014).

[7] Barrack Obama, "Executive Order 13636: Improving Critical Infrastructure Cybersecurity," February 12, 2013, available at: *https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity*

[8] Andy Ozment, NPPD Office of Cybersecurity and Communications Assistant Secretary, "Emerging Threats and Technologies to Protect the Homeland," Testimony before the House Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Security Technologies hearing, February 12, 2015.

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

incidents. Senator Christopher Coons from Delaware pointed out, "The bill would allow the Guard to respond to cyber disasters just as it does to natural disasters."[9] In an address to the National Governors Association, Colorado Governor John Hickenlooper stated "the National Guard should be mobilized to support federal and state efforts to protect critical infrastructure networks and respond to cyber incidents."[10] In the 2015 National Defense Authorization Act, the National Guard has now been authorized to establish more cyber mission teams (11 Army and 12 Air Guard), primarily to defend critical cyber networks against attacks from adversaries.

The National Guard forces can be activated for federal service under Title 10 US code or to perform state service under Title 32 US code. The dual status of the National Guard forces makes them a distinctive state homeland defense asset with direct access to Department of Defense (DoD) classified threat information and a national level multi-agency collaboration network. With federal funding, the National Guard Cyber Mission Forces are able to maintain their skills through participation in DoD sponsored exercises such as Cyber Guard which focuses on cyber defense of critical infrastructure. The National Guard force is 75 percent part-time military members who work full-time in the civilian workforce. This means many of the cyber defender guardsmen likely work in some of the critical infrastructure industries.

The government is unable to use federal military forces to enforce civil laws under the Posse Comitatus Act. However National Guard forces operating under the state authority of Title 32 are exempt from Posse Comitatus Act restrictions. Title 32 Section 902 authorizes the Secretary of Defense to "provide funds to a Governor to employ National Guard units or members to conduct homeland defense activities that the Secretary determines to be necessary and appropriate."[11] Even though most of the funding for National Guard equipment and training comes from federal sources, National Guard personnel and equipment are not "federalized" and therefore are available to the Governor in state or local emergencies.[12] The statute defines "homeland defense activities" as activities "undertaken for the military protection of the territory or domestic population of the United States, or of the infrastructure or other assets of the United States determined by the Secretary of Defense as

---

[9] William Matthews, "Cyber Uncertainty."
[10] Ibid
[11] US Code Title 32 Chapter 9 Section 902, "National Guard: Homeland Defense Activities: Definitions," available at: *https://www.law.cornell.edu/uscode/text/32/902*
[12] Maj. Gen. Timothy J. Lowenberg, "The Role of the National Guard in National Defense and Homeland Security," *National Guard Association of the United States,* no date, available at: *http://www.ngaus.org/sites/default/files/pdf/primer%20fin.pdf* .

being critical to national security, from a threat or aggression against the US."[13]

In many states, the Director of Homeland Security is the Lieutenant Governor who can recall troops to provide critical infrastructure defense through state funded or federal funded roles. Washington is one state whose government has established a critical infrastructure cyber defense capability in its National Guard network warfare units.[14] Washington state government statutes assign the state's emergency management to the Adjutant General and military department of the state which oversee cyber incidents threatening state or national security. They also offer their private and public utilities providers free penetration analysis and vulnerability assessments through partnerships to collectively defend those networks controlling critical infrastructure assets.

Currently Maryland, Michigan and California also have National Guard cyber mission forces and are developing frameworks to use those forces in a state role to defend critical infrastructure with private industry. In California, a joint Computer Network Defense Team performs vulnerability assessments, risk identification, incident response and other services for state agencies free of charge. The state also has an Air Guard Network Warfare Squadron that can be called on by the governor to test the security of state networks.[15]

In Maryland, the Air National Guard Network Warfare Squadron performs security assessments on state computer networks. The squadron teams with state agencies to launch simulated attacks against state networks. When they succeed, the squadron helps develop countermeasures to block future attacks.[16] These are the type of partnerships that many other state governments are wanting to develop with trained cyber defenders who can aid in thwarting the constant evolving threat posed on the most critical and vulnerable networks; however, federal appropriations have limited the current number of cyber forces.

[13] US Code Title 32 Chapter 9 Section 901, "National Guard: Homeland Defense Activities: Definitions," available at: *https://www.law.cornell.edu/uscode/text/32/901*
[14] A. Kambour, "Enhancing the Cybersecurity of Energy Systems and Infrastructure."
[15] William Matthews, "Cyber Uncertainty."
[16] Ibid

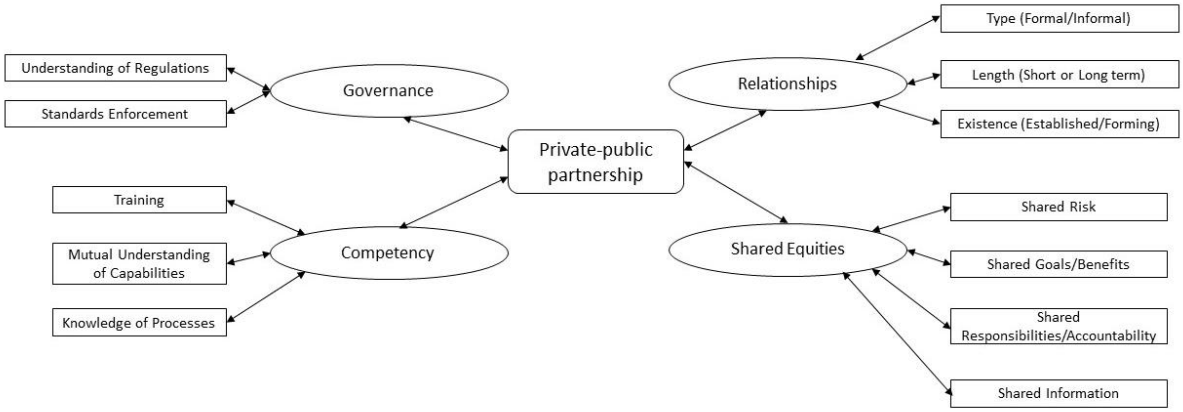
http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

Critical Infrastructure Cyber Defense Model Based on Private-Public Partnership Concept

For a number of years the US government has been stressing the importance of government and private industry to work together in partnerships in order to secure this nation's critical infrastructure. This need for private-public cyber defense partnerships is a thread which has carried through the 2002 *National Strategy to Secure Cyber Space*, and continues through the 2006 *National Infrastructure Protection Plan (NIPP)* and President Obama's 2009 *Cyber Space Policy Review*.[17] One can therefore deduce that cyber defense in critical infrastructure protection depends heavily on effective private-public partnerships (PPPs).

Our literature review and interviews with National Guard and Department of Homeland Security (DHS) cyber defense teams and private critical infrastructure providers exposed four recurring key features for effective PPPs: relationships, competency, shared equities and governance. We combined these aspects into a model that constitutes successful critical infrastructure cyber defense (see Figure 1).

Figure 1: Critical Infrastructure Cyber Defense Model



While trust is not explicitly included in the model, three of the four main factors in the model relate to trust. However, according to academic literature, trust takes time to develop in a partnership and is multi-faceted.[18] In his testimony before the House subcommittee on cybersecurity, Andy Ozment of NPPD pointed out that if public-private trust is broken, the open

[17] Larry Clinton, "A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense," *Journal of Strategic Security* 4: 2 (2011): 98, available at: *http://dx.doi.org/10.5038/1944-0472.4.2.6*.
[18] Nathan E.Busch, , and Austen D. Givens, "Public-Private Partnerships."

information exchange critical to the Cyber Information Sharing and Collaboration Program, which provides a trusted information sharing environment for private sector partners to share information and collaborate on cyber security threats, will not occur.[19] We now further explore the role of each model feature.

Relationships

Relationships between the private and public organizations play a key role in the partnership, and the length of time those relationships have been established ties to the trust level between partners. The length of time and amount of interaction within previously established relationships amongst partner organizations can also impact the amount of time necessary to establish trust.[20] Having those trusting working relationships in place is helpful during routine operations, but invaluable during crisis.[21]

Emerging National Guard cyber mission forces can learn from various cyber defense partnerships. For example, USCYBERCOM cyber defense teams work with private defense contractors in the Defense Industry Base critical infrastructure sector to develop private-public partnerships to defend critical information networks. The DHS NCCIC US-Cyber Emergency Response Team (US-CERT) and ICS-CERT partner with private critical infrastructure industry for cyber defense, as do the four states with National Guard units who have already partnered with critical infrastructure providers to provide vulnerability assessments and penetration testing for cyber defense incident response and cooperative exercises.

Shared Equities

Prior research indicates that when trust is low, transaction costs rise, which inhibits information exchange.[22] Explicit strategies to address these perceptions of risk are critical to success when information exchange is required for effective collaboration.[23] Sharing threat information, vulnerability data, or incident reporting are good practices for cyber defense

[19] Andy Ozment, “Emerging Threats and Technologies to Protect the Homeland.”
[20] Sharon S.Dawes, , Anthony M. Cresswell, and Theresa A. Pardo, "From “Need to Know” to “Need to Share”: Tangled Problems, Information Boundaries, and the Building of Public Sector Knowledge Networks," *Public Administration Review* 69:3 (2009): 397.
[21] Nathan E.Busch and Austen D. Givens, “Public-Private Partnerships.”
[22] Candace Jones, William S Hesterly, and Stephen P Borgatti, “A General Theory of Network Governance Exchange Conditions and Social Mechanisms,” *Academy of Management Review* 12:4(1997): 911.
[23] Sharon S. Dawes, Anthony M. Cresswell, and Theresa A. Pardo, “From ‘need to know’”.

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

of critical infrastructure and partnerships as well.[24] However, sometimes allowing information to be shared anonymously can facilitate a more open information exchange environment.

The DHS understands how crucial information sharing within a partnership between federal agencies and private entities is to effective critical infrastructure cyber defense.[25] According to a DHS US-CERT representative, one of the keys to establishing trust and open information exchange is the cooperative research and development agreements established with their cyber defense partners.[26] Those collaboratively produced documents ensure that the private industry critical infrastructure cyber defense partner understands the information voluntarily shared in the partnership will only be used to enhance its cyber defense and will not be shared with regulatory agencies in accordance with the Critical Infrastructure Information Act.[27] Many private critical infrastructure providers are currently unaware that those protections exist which leads to a reluctance to voluntarily share cyber incident or vulnerability information.[28]

Competency

An organization's competency and a partner's perception of how competent that organization is also add to the trust equation in a partnership. An organization's competency can be measured by others through the skill level of its employees, the organization's external reputation, its leadership practices and the organization's internal processes.

Competency of an organization in a private-public partnership can also include its ability to safeguard information. The DHS has established the Protected Critical Infrastructure Information (PCII) program based on information protection legislation in the 2002 Critical Information Act. PCII protections mean that homeland security partners can be confident that

---

[24] European Network and Information Security Agency, "Cooperative Models for Effective Public Private Partnership: Good Practice Guide," available at: *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/national-public-private-partnerships-ppps/good-practice-guide-on-cooperatve-models-for-effective-ppps*.
[25] Andy Ozment, "Emerging Threats and Technologies to Protect the Homeland."
[26] Interview with Department of Homeland Security United States Computer Emergency Response Team representative, April 6, 2015.
[27] Department of Homeland Security Protected Critical Infrastructure Information homepage, updated June 18, 2014, available at: http*://www.dhs.gov/protected-critical-infrastructure-information-pcii-program*.
[28] Interview with Department of Homeland Security United States Computer Emergency Response Team representative, April 6, 2015.

sharing their information with the government will not expose sensitive or proprietary data.[29] Even though government cyber defense organizations are bound to protect collected information and not share it with regulatory agencies, many private organizations in partnerships still do not have a feeling of sustained trust.[30] This feeling of distrust could also result from private critical infrastructure companies' lack of understanding of what protections the Critical Information Act of 2002 and the PCII program afford with regard to the information they volunteer and what cyber defenders find.[31]

Competency can be developed and maintained through regular collaborative training exercises so that both sides of the partnership can better understand each other's capabilities. The Washington state emergency management division regularly runs collaborative cybersecurity and defense tabletop exercises with state government leadership, state emergency management, National Guard cyber mission forces, and private critical infrastructure providers in order to comprehend the severity of cyber threats, and practice methods to mitigate those threats.

Cyber Guard is a joint cyberspace training exercise focused on national defensive cyberspace operations whole-of-government approach with a state response and a larger federal response to significant cyberattacks on critical infrastructure. This annual exercise brings together National Guard, CYBERCOM, DHS, FBI and state Joint Operations Centers in order to better understand each other's capabilities and processes.[32] Participation in these training exercises by private and public organizations could also help develop trust and encourage private-public partnership participation for cyber defense through better understanding of each organization's competency. Securing ICS protocols on industry networks requires specialized training and certifications separate from defending an industry's information networks. Cyber Guard focuses on developing knowledge and joint processes to be competent to defend those types of systems.

---

[29] Department of Homeland Security, "Protected Critical Infrastructure Information Program Fact Sheet," July 2014, available at: *http://www.dhs.gov/sites/default/files/publications/PCII-Fact-Sheet-2014-508.pdf*.
[30] Department of Homeland Security Integrated Task Force, "Evaluation of Existing Public-Private Partnership Model," July 12, 2013, available at: *https://www.chicagofirst.org/resources/dhs_partnership_report.pdf*.
[31] Interview with Department of Homeland Security United States Computer Emergency Response Team representative, Apr 6, 2015.
[32] US Cyber Command, "Cyber Guard 13-1 After Action Report," Feb 7, 2014.

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

In 2012, the Michigan state government partnered with academia and industry to create a public-private cyber range because they felt that would help improve cyber defense competency between their National Guard cyber mission teams and the private sector. Michigan Chief Information Officer hopes the cyber exercise range will strengthen the state of Michigan's cyber-readiness and foster stronger private-public partnerships for cyber defense of critical infrastructure.[33]

Governance

Governance in critical infrastructure cyber defense currently mandates that government agencies share information on cyber threat data, guidelines, and best practices; however, information sharing by private critical infrastructure providers is voluntary. Regulations do exist, requiring critical infrastructure networks to be in compliance with reliability standards set by regulatory organizations. The subject then becomes how understandable and enforceable the regulations and mandatory standards are. If one government agency is charged to enforce those mandatory standards, what keeps a non-regulatory government agency such as a National Guard cyber mission team from turning in a non-compliant private partner for that non-compliance? This returns to the issue of partners understanding each other's processes, particularly with regard to handling and protecting sensitive information and only providing that information to those with a legitimate need to know.

Due to the increasing threat of cyber incidents to cause significant damage to critical infrastructure, some states have passed legislation to better defend critical infrastructure from cyberattack and drafted cyber annexes to their state emergency action plans. The state of Washington's cyber annex to their state emergency action plan designates the state Homeland Security Advisor as the lead for any significant cyber incident. That state Homeland Security Advisor coordinates the cyber incident response with the help of state Cyber Unified Coordination Group consisting of various state government cyber security officials, law enforcement, cyber academia, the lead National Guard cyber planner, and private industry critical infrastructure key resources representatives.[34]

---

[33] Colin Wood, "Cybersecurity Gets a Boost from the National Guard," *Emergency Management*, March 3, 2014, available at: *http://www.emergencymgmt.com/safety/Cybersecurity-National-Guard.html?page=1*.
[34] State of Washington, "Washington State Significant Cyber Incident Annex to the Washington State Comprehensive Emergency Management Plan: Annex D," March 4, 2015: 7-8, available at: *http://mil.wa.gov/uploads/pdf/PLANS/wastatesignificantcyberincidentannex20150324.pdf*.

Research Method

Yin's methods[35] were followed to perform a single case study of critical infrastructure cyber defense to validate the key aspects of effective PPPs highlighted in the literature review and initial interviews. Another goal of the case study was to discover how emerging National Guard CMTs could build effective PPPs by focusing on the main aspects of the critical infrastructure cyber defense model. Our units of analysis were four current and future cyber defenders from National Guard and DHS and five public/private critical infrastructure providers. We used the four main factors of relationships, competency, shared equities and governance, from our model as our propositions to study (see Attachment 1) and developed a questionnaire (see Attachment 2) as a mechanism to link data to the propositions and interpret findings. All respondents answered the same set of questions. Some of the respondents have performed critical infrastructure cyber defense in response to actual cyber incidents and others have performed cyber defense as a partner organization during Cyber Guard training exercises.

Discussion

Through interviews and questionnaire responses, the overarching theme that resounded throughout Subject Matter Expert (SME) responses was that PPPs are very important for an effective critical infrastructure cyber defense. An effective PPP cannot exist unless mutual trust is established between the partner organizations and relationships are key to establishing that trust. Both federal government and private industry officials stated that those relationships and the necessary trust building takes time and is typically only effective with personal contacts between the organizations.[36] Most respondents felt having a liaison in their partner organizations would improve the effectiveness of the critical infrastructure cyber defense partnership. Only one public critical infrastructure provider felt liaisons would not improve cyber defense partnerships and that was the only respondent who stated he/she currently utilizes liaisons. This response clearly emphasizes the need to better understand and develop the role of an effective liaison in PPPs.

Most of the respondents from both private and public felt that transparent information exchange is an important factor for cyber defense partnerships.

---

[35] Robert K. Yin, "Case Study Research: Design and Methods,"*Sage Publications*, 2013: 28-29.

[36] Interview with Department of Homeland Security United States Computer Emergency Readiness Team representative, April 6, 2015.

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

Currently private critical infrastructure providers are eager to receive government provided cyber threat information; however, many, especially those large enough to provide internal cyber defense for their networks, are reluctant to openly reciprocate that information exchange. Most private critical infrastructure providers are worried the government agency providing the cyber defense support will turn their voluntarily shared network vulnerability data over to a regulatory government agency.[37] National Guard critical infrastructure cyber defenders need to give special attention to those information protection concerns. These concerns warrant taking the time to communicate with critical infrastructure providers how data observed during vulnerability analysis and other cyber defense activities is protected by the Protected Critical Infrastructure Information Act. Dealing with that concern in this manner should help build more trust since all respondents to the questionnaire felt knowledge of their partner organization's information protection procedures would promote information exchange rather than impede it. Implementing a practice similar to the DHS written cooperative trust agreements could address that concern and strengthen partnership trust.

Both sides agreed security classification of cyber threat data was a common impediment to information exchange. One critical infrastructure provider pointed out it is difficult to convince management to implement different, sometimes costly, security practices when one is not able to share the threat information with them. It would also be helpful to know which cyber threat information can be shared with other government organizations within the partnership because that is not always clear.[38] One way DHS has dealt with that issue is by using state protective security advisors to work with and sponsor private infrastructure providers for security clearances.[39] The National Guard should use close community ties to provide that same service to help bridge the gap between government providers of cyber threat data and private critical infrastructure providers.

All respondents except for one National Guard cyber defender felt it was important that legislation, standards and policies are easy to interpret. However, four out of the five critical infrastructure providers and one out of three National Guard cyber defenders felt current standards are easy to

[37] Interview with anonymous critical infrastructure provider representative, April 9, 2015.
[38] Interview with local Omaha critical infrastructure provider cybersecurity representative, April 22, 2015.
[39] Interview with Department of Homeland Security United States Computer Emergency Readiness Team representative, April 6, 2015.

implement. National Guard cyber teams should be prepared to act as interpreters of standards and policies.

Another way the National Guard cyber teams can bridge the gap between government agencies and the public-private critical infrastructure providers is acting as a fusion cell to interpret the many government cyber threat feeds and filter out the most serious threats to critical infrastructure providers. As a fusion cell for cyber threat analysis, the National Guard cyber teams could also provide forensics of the thousands of malware attacks critical infrastructure providers face and interpret which attacks are malicious and severe enough to recommend spending resources to defend against them.[40]

Interestingly, most of the respondents felt their own personnel did not have the necessary expertise and training for critical infrastructure cyber defense. National Guard cyber teams should be aware that a majority of the partners see joint cyber defense training exercises, such as Cyber Guard, as important for improving cyber defense partnership capabilities. Most respondents are interested in third parties such as local universities providing mock ICS/SCADA networks or Michigan's state-wide cyber range as mediums for that collaborative joint training. National Guard cyber teams should investigate these third party training opportunities to help forge effective cyber PPPs.

Some threats to the validity of our findings were the short amount of time allowed for this study, only three months, and the small sampling of SMEs available to answer the questionnaire. Future studies should attempt to question more subjects from a variety of critical infrastructure providers.

Conclusions

More remote access to industry information technology systems has made the ICS protocols which regulate daily operations on the nation's critical infrastructure cyber networks more vulnerable to outside attack. Federal and state governments have always had the authority to use National Guard forces to physically defend critical infrastructure and key resources vital to the nation's interests and way of life. Many state governments feel cyber defense of the networks controlling that critical infrastructure is not much different, which makes cyber defense of critical infrastructure a lucrative role for the National Guard cyber mission forces that state governments are working to

[40] Interview with local Omaha critical infrastructure provider cybersecurity representative, April 22, 2015.

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

develop. Due to the privatization of most of the nation's critical infrastructure, the National Guard CMTs will have to develop effective private-public partnerships with those private industries in order to be successful in this new mission set vital to our nation's security. Based upon this case study, the critical infrastructure cyber defense model provides a good guide for National Guard cyber mission teams to reference when developing private-public partnerships to perform their mission effectively. National Guard CMTs should build upon their current community relationships to establish written agreements with critical infrastructure partners to develop the underlying trust that encourages information sharing. They should also use those same community relationships with academia and industry to create third party training networks for all partners to promote a collaborative learning environment for a more effective critical infrastructure cyber defense and stronger trusting partnerships.

Appendix 1. Case Study Propositions

Proposition Categories	Propositions
1. Relationships	Having an established relationship between private and public partners, no matter the type, builds trust which leads to a more effective mission than only assembly the partnership in crisis
	1.a. Whether partner relationships are formal or informal does not matter, but rather is the existence of a relationship affects trust.
	1.b. Long term relationships with frequent partner interaction establish a more effective partnership than reactionary short term crisis relationships.
	1.c. Previous existence of a relationship between partner organizations leads to more trust established.
2. Shared Equities	The partners in the cyber defense private-public partnership must share some equities to establish and maintain trust.
	2.a. There is a sense of shared goals and benefits. Partners depend upon each other to accomplish these common goals.
	2.b. Risk should be evenly shared amongst the partners in order to establish trust.
	2.c. Free exchange of information is critical to an effective cyber defense partnership. Trust between partners is critical for this information sharing to occur.
	2.d. Evenly distributed and understood responsibilities and accountability amongst the cyber defense partnership are important to establish trust.
3. Competency	The ability for partners to perform their responsibilities competently.
	3.a. Knowledge of partner's cyber defense capabilities is critical to developing trust in the partnership.
	3.b. Both sides of the private-public partnership are lacking proper training to effectively perform cyber defense mission and require knowledge from their partner organization.
	3.c. Knowledge of partner's cyber defense and information protection processes are important to establish and maintain partnership trust.
4. Governance	Compliance standards and regulations for critical infrastructure providers are necessary for effective cyber defense.
	4.a. Legislation and standards must be easily understood in order to effectively be implemented.
	4.b. Mismatched information sharing (required for government

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

	agencies and voluntary for private/public critical infrastructure companies) hampers the partnership.

Appendix 2. Questionnaire Relationship to Propositions

	Propositions correlated to Questionnaire Questions															
Questions	1	1a	1b	1c	2	2a	2b	2c	2d	3	3a	3b	3c	4	4a	4b
Q1: Are you aware of any private-public (govt) partnerships in your organization for cybersecurity?	X	X	X	X												
Q1.1 Please select the nature of those private-public partnerships for cyber defense (you may choose multiple answers). Formal, informal, long-term, short-term																
Q1.2: Are these partnerships documented in a memo of agreement or joint policies?	X	X	X	X										X		
Q1.3 How many cyber defense partnerships does your organization currently participate in?	X															
Q1.4 How important are private-public partnerships for effective critical infrastructure cyber defense?	X					X				X						
Q2: Do you think having a liaison in a partner's organization would improve a cyber-defense partnership?	X					X	X	X	X		X					
Q2.1: Does your organization currently have a liaison position for coordinating cyber defense activities?	X					X	X	X	X		X					

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

Q3 How much does the cyber defense competency of the partner organization matter for your responsibilities to protect key critical infrastructure elements?	X									X						
Q3.1 How important is it to know about the cyber defense capabilities a partner organization can provide?	X									X	X					
Q3.2 Provide some examples of desirable capabilities?											X					
Q3.3 How important is it that your cyber defense partner organization participates in ongoing cyber defense training to maintain current knowledge and skills?										X		X				
Q3.3.1 Do you feel your own personnel have the necessary expertise and training to defend critical infrastructure networks?										X		X	X			
Q3.4 How important are joint training exercises/practice for cyber defense or incident response be for improving mutual awareness of capabilities?						X				X	X	X				
Q3.5 How desirable would it be to have a third party (e.g.												X				

University) provide a mock Industrial Control Systems network for cyber defense education and training?																
Q4 How important do you think it is to share transparently, with attribution, all pertinent information (vulnerabilities, incidents, threat information) with other partners for an effective cyber defense partnership?					X			X								
Q5 Would you be more willing to share information cyber defense information (threat, vulnerabilities, attack trends, etc.), if shared anonymously?					X			X								
Q6 Rate the following issues for their ability to hamper information sharing: 1. Security Classification of cyber threat information, 2.Disclosure of previously known vulnerabilities, 3. Private industry competitive edge, 4. Collaboratively developed information sharing agreements between public and private partners, 5. Ability to anonymously share information, 6. Knowledge of partner's					X			X								

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

cyber defense capabilities, 7. Knowledge of cyber defense partner's information protection practices, 8. Attribution tied to information source, 9. NIST standards for critical infrastructure cyber defense																
Q6.1 Are there any other factors that influence information sharing in a cyber-defense partnership?					X			X								
Q7 How important is it to understand the methods for protecting sensitive information used by your partner organization in a cyber-defense partnership ?								X					X			
Q7.1 Your organization has established procedures for protecting sensitive information pertaining to critical infrastructure cyber defense? (Disagree/Agree)								X					X	X		X
Q7.1.1 Other organizations in your cyber defense partnership are familiar with your sensitive information protection policies and methods. (Disagree/Agree)								X			X		X	X		X

Q7.2 I trust the organizations in a cyber-defense partnership for their ability to provide the same level of protection for sensitive information. (Disagree/Agree)										X			X			
Q8 Voluntary requirements for private companies to share cyber defense information are sufficient for effective cyber defense of critical infrastructure. (Disagree/Agree)								X						X		X
Q8.1 There should be more legislation for private companies mandating sharing of cyber defense information with relevant partners? (Disagree/Agree)								X						X		X
Q9: How important are the following aspects to establishing/maintaining an effective critical infrastructure cyber defense partnership? 1. Share Risk, 2. Incentives, 3. All cyber defense partners share common cyber defense goals, 4. All cyber defense partners understand their own organization's cyber defense roles and responsibilities, 5. All cyber defense partners understand each other's					X	X			X		X		X			

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441

cyber defense roles and responsibilities, 6. All cyber defense partners are held equally accountable to their responsibilities in the partnership																
Q9.1 Should this risk be evenly distributed across the partner organizations?					X		X									
Q9.2 What are some incentives that will likely improve participation in cyber defense private public partnerships?								X								
Q10. How important are outsourced cyber security activities are effective for critical infrastructure cyber defense	X					X			X							
Q10.1 State sponsored Cyber Protection Teams are equally effective for critical infrastructure cyber defense. (Disagree/Agree)	X					X			X							
Q10.1.1 What are some reasons for your response?	X					X			X							
Q11. How important to critical infrastructure cyber defense are easily interpreted legislation and policies? .													X	X	X	
Q11.1 I believe current regulatory penalties for non-compliance with critical infrastructure cyber network standards														X		X

are sufficient for critical infrastructure providers. (Disagree/Agree)																
Q11.2 National Institute of Standards and Technology standards for critical infrastructure cyber defense are easy to implement. (Disagree/Agree)														X		X

http://scholarcommons.usf.edu/jss/vol8/iss4/1
DOI: http://dx.doi.org/10.5038/1944-0472.8.4.1441