Journal of Strategic Security

Volume 4
Number 2 *Volume 4, No. 2, Summer 2011: Strategic Security in the Cyber Age*

Article 7

A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense

Larry Clinton
Internet Security Alliance Washington, D.C., USA, lclinton@isalliance.org

pp. 97-112

Recommended Citation
Clinton, Larry. "A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense." *Journal of Strategic Security* 4, no. 2 (2011): : 97-112.
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6
Available at: https://scholarcommons.usf.edu/jss/vol4/iss2/7

A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense

Author Biography

Larry Clinton is President and CEO of the Internet Security Alliance (ISA). ISA represents major corporations from the Aviation, Banking, Communications, Defense, Education, Financial Services Insurance, Manufacturing, Technology and Security industries. ISA's mission is to integrate advanced technology with economics and public policy to create a sustainable system of cyber security. Mr. Clinton is one of the clearest voices on cyber security and has been featured in mass media such as USA Today, PBS News Hour, The Morning Show (CBS), Fox News, CNN, CSPAN, and CNBC. He has also authored numerous professional journal articles on cyber security as well as being a past guest editor for the Cutter IT Journal. Mr. Clinton is regularly called upon to testify before both the U.S. House and Senate. In 2008, ISA published its Cyber Security Social Contract which is both the first and last source cited in the Executive Summary of President Obama's Cyber Space Policy Review, which also cited more than a dozen ISA white papers—far more than any other source.

Abstract

Cyber security is a complex issue that requires a smart, balanced approach to public-private partnership. However, there is not a simple gold standard or mandatory minimum standard of cyber security, which can cause friction in the relationship between government and private industry. There are fundamental differences in these two unevenly yoked partners: government's fundamental role under the U.S. Constitution is to provide for the common defense; industry's role, backed by nearly a hundred years of case law, is to maximize shareholder value. Further differences are that government partners and industry players often assess risk differently, based on their differing missions and objectives. To be successful, both government and industry need to remain committed to the relationship and continue working on it by understanding the complexity of the situation, adapting where appropriate to their partner's perspective. For the public-private partnership to endure and grow, an appreciation of these differing perspectives—born from different legally mandated responsibilities—must be reached. Ultimately, the government should compensate private entities for making investments that align with the government's perspective, such as the social contract, rather than mandating that the shareholders subsidize the government function of providing for the common defense.

Journal of Strategic Security
Volume IV Issue 2 2011, pp. 97-112
DOI: 10.5038/1944-0472.4.2.6

JSS
Published Quarterly by Henley-Putnam University Press
with support from the University of South Florida Libraries

A Relationship on the Rocks: Industry-Government Partnership for Cyber Defense

Larry Clinton
Internet Security Alliance
Washington, D.C., USA
lclinton@isalliance.org

Abstract

Cyber security is a complex issue that requires a smart, balanced approach to public-private partnership. However, there is not a simple gold standard or mandatory minimum standard of cyber security, which can cause friction in the relationship between government and private industry. There are fundamental differences in these two unevenly yoked partners: government's fundamental role under the U.S. Constitution is to provide for the common defense; industry's role, backed by nearly a hundred years of case law, is to maximize shareholder value. Further differences are that government partners and industry players often assess risk differently, based on their differing missions and objectives. To be successful, both government and industry need to remain committed to the relationship and continue working on it by understanding the complexity of the situation, adapting where appropriate to their partner's perspective. For the public-private partnership to endure and grow, an appreciation of these differing perspectives—born from different legally mandated responsibilities—must be reached. Ultimately, the government should compensate private entities for making investments that align with the government's perspective, such as the social contract, rather than mandating that the shareholders subsidize the government function of providing for the common defense.

Introduction

In presenting the annual threat assessment to Congress in 2010, U.S. Director of National Intelligence Dennis Blair said:

> "The national security of the United States, our economic prosperity and the daily function of our government are dependent on a dynamic public private information infrastructure which includes telecommunications, computer networks and systems and the information residing within. This critical infrastructure is severely threatened...I am here today to stress that acting independently, neither the U.S. Government nor the private sector can fully control or protect the country's information infrastructure. Yet, with increased national attention and investment in cyber security initiatives, I am confident the United States can implement measures to mitigate this negative situation."[1]

In stressing the need for industry and government to work together Mr. Blair, has simply repeated the U.S. Government mantra that dates at least to the 2002 *National Strategy to Secure Cyber Space*,[2] and continues through the 2006 *National Infrastructure Protection Plan (NIPP)* and President Obama's 2009 *Cyber Space Policy Review* which all attest that, at least for cyber security,[3, 4] government and industry need to operate as partners.

However, frustration with the persistence of the cyber threat has led some to question whether this marriage can survive. An alternative might be a more paternalistic model wherein government dictates to industry what it believes ought to be done to secure cyber space and to enforce these mandates with heavy penalties. This article will examine the current state of the pubic-private partnership for cyber security and some of the proposals to redefine it. It also will consider whether the current partnership could become more effective by adopting some principles from the literature on effective relationships.

The Once and Future Partnership

The 2002 National Strategy envisioned a partnership of equals wherein industry was expected to develop technologies, standards, and practices to secure expanding cyber networks. Government's role with respect to the private sector was largely confined to education, international coordination, and assisting with R&D. The strategy envisioned market efficiencies as sufficient to drive the adoption of protective measures.

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

In the NIPP in 2004, the partnership was still envisioned as one of peers, although there was a greater definition of how the roles between the partners would need to be managed:

> "The success of the public private partnership depends on articulating mutual benefits to government and the private sector partners. While articulating the value proposition to the government typically is clear, it is often difficult to articulate the benefits of participating to the private sector.... In assessing the value proposition for the private sector, there is a clear national security and homeland security interest in ensuring the collective protection of our nation's [critical infrastructure/key resources] CI/KR. Government can engage industry to go beyond efforts already justified by their own corporate business plans to assist in broad scale CI/KR protection through activities such as:
>
> - Providing owners and operators timely analytical accurate and useful information...
> - Ensuring industry is engaged as early as possible in the development of initiatives and policies related to the NIPP...
> - Articulating to corporate leaders ...both the business and national security benefits of investing in security measures that go beyond their business case...
> - Creating an environment that encourages and supports incentives to voluntarily adopt widely accepted sound security best practices....
> - Providing support for research needed to enhance future CI/KR protection efforts."[5]

Finally, the *Cyber Space Policy Review* claimed that while the foundation of the relationship seemed unchanged, the need for the government to be more proactive in working with industry was apparent:

> "The government, working with State and local partners, should identify procurement strategies that will incentivize the market to make more secure products and services available to the public. Additional incentive mechanisms that the government should explore include adjustments to liability considerations (reduced liability in exchange for improved security or increased liability for the consequences of poor security), indemnification, tax incentives, and new regulatory requirements and compliance mechanisms."[6]

To many, this proposition seems axiomatic. Since industry owns, operates, and, in fact, creates, the vast majority of the information networks that make up cyber space, and government operations are reliant on these private networks, securing them must be through a partnership. This is especially true since, as several of the aforementioned national policy documents point out, the government is looking for private investment in cyber security that may exceed an enterprise's commercial needs.[7]

Problematic Relationships

Partnerships between people, or businesses or government can be more difficult than one might expect. Lack of coordination of the partners' roles, responsibilities and expectations can lead to problems even when the partners in the relationship appear to have broadly aligned goals. Communication about these potential differences can be problematic, even if both partners in the relationship sincerely want the partnership to succeed.

Social exchange theory postulates that people enter into relationships based on the perception that rewards will outweigh costs.[8] When costs outweigh rewards, people will seek other alternatives that are more beneficial. If there are no better alternatives, people may stay in costly relationships, but feel less committed to them and behave in ways that do not enhance the long-term effectiveness of the relationship.

In the case of the public-private partnership to create a secure cyber system, it is unlikely that the private sector, at least writ large, can or will actually withdraw from their partnership with the government. However, a partnership that assumes static traditional roles and does not create tangible perceived rewards on the part of both parties could create a dysfunctional relationship lacking in commitment and proactive behavior. If such a relationship emerged, it could lessen overall security, which could have catastrophic consequences. Thus, with respect to cyber security, the management of the partnership itself may have more strategic significance than any of the more talked about operational or technical issues.

Signs of Trouble

To implement the public-private partnership for cyber security the Department of Homeland Security (DHS) created a series of "sector coordinating councils," each of which would have corresponding government

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

coordination councils. The basic idea was that these groups would work together to develop plans and procedures to implement the goals of the partnership.

Reviews of the partnership from the Government Accountability Office (GAO) have been generally less than flattering. One example is their 2009 report "Critical Infrastructure Protection Report: Current Cyber Sector Specific Planning Approach Needs Reassessment," which found:

> "Although DHS reported many efforts under way and planned to improve the cyber content of sector-specific plans, sector-specific agencies have yet to update their respective sector-specific plans to fully address key DHS cyber security criteria. For example, of the 17 sector-specific plans, only 9 have been updated. Of these 9 updates, just 3 addressed missing cyber criteria, and those 3 involved only a relatively small number (3 or fewer) of the criteria in question…the continuing lack of plans that fully address key cyber criteria has reduced the effectiveness of the existing sector planning approach and thus increases the risk that the nation's cyber assets have not been adequately identified, prioritized, and protected. The lack of complete updates and progress reports are further evidence that the sector planning process has not been effective and thus leaves the nation in the position of not knowing precisely where it stands in securing cyber critical infrastructures. Not following up to address these conditions also shows DHS is not making sector planning a priority. Further, recent studies by a presidential working group…also identified shortfalls in the effectiveness of the current public-private partnership approach."[9]

Other commentators, perhaps lacking the GAO's institutional imperative for dispassion have been less genteel. For example, in 2011 Jim Lewis of the Center for Strategic and International Studies (CSIS) updated the *CSIS Commission on Cyber Security's* 2008 report by concluding:

> "The cyber security debate is stuck. Many of the solutions still advanced for cyber security are well past their sell by date. Public-private partnerships, information sharing and self-regulation are remedies we have tried for more than a decade without success. We need new concepts and new strategies if we are to reduce the risk in cyber space to the United States."[10]

Redefining the Public-Private Partnership

For some the alternatives appear clear. Either we follow the *laissez faire* path advocated in the *National Strategy to Secure Cyber Space* or we move to a regulatory model, and their preference is clear—government regulation:

> "Identifying progress in 2011 will be simple. If the nation passes laws and the administration issues effective regulations for critical infrastructure there has been progress. These should include mandatory improvements in authentication of identity for critical infrastructure. No regulations mean inadequate progress."[11]

While the dominant pattern of the industry-government partnership remains basically as outlined in the *National Strategy* released in 2002, there are more recent legislative initiatives that seek to redefine the relationship away from the notion of peers working together toward one more akin to a strict parent overseeing their child's homework.

One example of this strict hierarchical, paternal model is apparent in the so called "combined bill," which was drafted under the auspices of Senate Majority Leader Harry Reid's office as an attempt to merge competing comprehensive cyber security bills that emerged from the Senate Homeland Security and Commerce Committees in late 2010. This bill would have defined components of "covered critical infrastructure" subject to federal cyber security mandates with a new compliance regime including penalties for noncompliance. The bill defined this new partnership this way:

> "The bill creates a dynamic partnership between the government and private sector in which the private sector is responsible for enhancing security of the Nation's most critical systems while the government ensures effective oversight and compliance."[12]

This construction would appear to be a somewhat strained definition of a "partnership;" gone is the notion of the partners working together to solve problems. Instead, there is the assertion that industry must perform and government must judge. The notion of understanding the needs of the separate partners and seeking a value proposition to make the relationship a rewarding one (this is consistent with Mead's notion of social exchange) is also absent, as are Baxter's ideas of a dynamic evolving partnership.[13] And, the bill contains little or none of the specific tax, procurement and liability or other incentives to spur private investment to fulfill broader national security goals as suggested in the *Cyber Space Policy*

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

Review. Instead, there is the comparatively simple assertion that industry will take on the role of providing national cyber security, and government will judge and enforce harsh civil penalties for lack of compliance.

To analogize this to a personal relationship, this type of relationship would be like one spouse saying to the other, "Honey, your job is going to be to do all the things necessary to secure our family. You will have to generate the money, buy the house, clean the house, pay the bills, buy the food, cook the dinner, have the kids, raise the kids, etc. My job will be to evaluate how well you do your job. And, of course, if you don't meet my specifications, there will be severe penalties." The partnership described in this construction is similar to a parent-child relationship, wherein the parent (government) feels the need to exhibit some tough love on an uncooperative and immature child (the private sector).

The analogy breaks down, however, when one realizes that in this case the "child" (industry) is actually far bigger, stronger, and has more resources than the supposed parent. Indeed, it is the parent (government) in this case that is ultimately reliant on the child for cyber security.

The notion that the private sector has been in some way unruly and needs to be disciplined by government is questionable. While industry cyber systems are vulnerable to attack—as are virtually all infrastructures historically—the market has produced an array of effective means to protect their cyber systems. The problem is the lack of proper implementation of cyber security best practices and relatively simple fixes, like software updates and security patches. Indeed, public statements from the CIA and the NSA are consistent with research from such organizations as PricewaterhouseCoopers,[14, 15, 16] Verizon, and the U.S. Secret Service,[17] which show that 80-94 percent of cyber events could be prevented or successfully mitigated by using standards practices and technologies that are already available on the market. The question becomes not what needs to be done, but how do we get people to do it? Will a traditional regulatory model work in this space, or does a newer model to address uniquely 21st century issues need to evolve?

The assumption that adopting a more paternalistic model of government regulatory mandates would be successful in resolving our cyber security issues is unsubstantiated. Cyber security provisions in laws like HIPPA and SOX have not been effective in securing the systems they apply to. Moreover, there are numerous reasons to believe government regulation may not work at all, some of which are outlined below.

Forging a Solution: More Government Regulation Is Not the Answer

Cyber security is a unique issue area that is especially difficult to address through the traditional federal regulatory structure. President Obama, who was one of the most pro-regulation members of the U.S. Senate during his tenure there, has observed that the interconnected nature of the Internet makes using regulations to secure it highly problematic.[18]

The underlying assumption of those who seek to regulate in this space is often that the technology is broken and simply needs to be brought up to code via regulatory mandates. In reality, the situation is not so much about faulty systems but that the incentives to attack the systems are so great. Virtually all the economic incentives currently favor those who are interested in conducting cyber attacks. Cyber attack methods can be acquired over the Internet. There are vast profits that can be made via cyber crime and the chances of being successfully prosecuted are virtually nil.

Moreover, the numbers of attractive targets for attack are virtually limitless, as defenses are almost inherently a generation behind the attackers and demonstrating return on investment for cyber defense is problematic since it's difficult to measure the effects of something that has been prevented from occurring.

Our problem may not be so much that the systems are built with exploitable flaws or negligently maintained, as it is that economic incentives to attack the systems are so massive that even the best systems may be subject to compromise. There is in fact a growing body of evidence that suggests that notwithstanding the technologies used, determined attackers, such as the highly sophisticated, well-funded and often state-sponsored attackers, the so called Advanced Persistent Threat (APT), will eventually succeed in compromising perimeter defenses.[19]

Even if regulation were desirable, whom should the government regulate? The vendors who make the systems or the users who purchase them and who may not follow the manufacturer's recommendations for keeping the software up-to-date and properly installed? Maybe the Internet service providers (ISP) who deliver the Internet traffic should be regulated or maybe all of the above?

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

Moreover, even if government could magically create an effective set of regulatory mandates, the technology changes so quickly that keeping the regulations current would be a daunting task especially given the cumbersome regulatory process which was designed to address the technology of the pre-digital age.

There is no assurance that government regulations if implemented would be effective. Regulatory processes tend to become adversarial quickly, and political pressure may be brought to bear to create a ceiling for acceptable behavior rather than the intended floor. Given this inherently political nature of the regulatory system, it is at least as plausible that the regulations that emerged would be watered down much as campaign finance regulations are. For example, virtually every politician in the nation is able to attest that they are in compliance with federal campaign funding regulations, yet almost no one believes that the intent of the regulations has been served by this compliance.

Additionally, there is the possibility that government proscribed mandates could turn out to be counterproductive. For example, some legislative proposals have called for dramatic increases in cyber security auditing. Repetitive auditing takes security people away from doing actual security and instead forces them to spend time on overly burdensome compliance. In one instance, a multi-state enterprise reported that whereas they once did quarterly penetration testing (a highly effective cyber security best practice), the growing audit requirements now only allowed them time and resources to do annual penetration testing—a 75 percent reduction in a security best practice because security resources were being diverted to regulatory compliance.

In a larger context, although cyber security is an important value, it is not the only value. Even if a set of regulatory mandates could work, they should be assessed in relation to their costs in terms of innovation, investment and job creation. A U.S. law would apply only to U.S. companies which are competing in a world market. While some industry is inherently tied geographically to the U.S., many industries, including defense, IT and manufacturing can and could become motivated to move their operations to less regulated locations if the cost of operation were driven up by security mandates, just as businesses traditionally move to lower cost states in the Union. Not only would this outcome be inconsistent with the need to create more jobs in the US, but the notion of driving IT and cyber security expertise off shore has other negative implications.

Journal of Strategic Security

Enrich the Public-Private Partnership, Don't Change It

Faced with a growing cyber security problem and dim prospects for success if the model is altered toward greater government control, an alternative approach would be to work on the government-industry relationship to make it stronger and more successful. This is the approach advocated by a group of major industry associations and civil liberties representatives who reviewed this subject at the conclusion of the 111th Congress and presented the following conclusions in a white paper:

> "The current critical infrastructure protection partnership is sound, the framework is widely accepted, and the construct is one in which both government and industry are heavily invested. The current partnership model has accomplished a great deal. However, an effective and sustainable system of cybersecurity requires a fuller implementation of the voluntary industry-government partnership originally described in the NIPP. Abandoning the core tenets of the model in favor of a more government-centric set of mandates would be counterproductive to both our economic and national security. Rather than creating a new mechanism to accommodate the public-private partnership, government and industry need to continue to develop and enhance the existing one."[20]

While the notion of industry and government attending "couples therapy" sessions is obviously impractical, there are a number of competencies that have been identified in literature dealing with successful human relationships that may be adaptable to the industry-government partnership for cyber security. Among the principles that could be instructive are complexity, perspective taking, and flexibility.[21]

Complexity

When humans enter into a voluntary relationship, it is usually based on an initial perceived similarity, such as mutual attraction, common interests, or occupation. Often people will make assumptions about each other assuming there will be other similarities that can be shared. In successful relationships, individuals come to recognize that the other is more complex, and this complexity must be managed if the relationship is to endure.[22] Individuals who do not appreciate the complexities of their partner often have less successful relationships.

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

The cyber security partnership similarly emerged out of a perceived common interest in protecting the networks the partners shared. Out of this mutual perception evolved the sector and government coordination councils and other similar bodies, which are designed to provide the structure for the relationship.

While government does indeed, at least at the federal level, operate in structures closely aligned to their coordinating councils (Treasury Department representing banking, Department of Defense representing defense, etc.), corporate investment in cyber security is not determined at this level. Cyber security investments and the adoption of best practices and standards are not run through industry sectors or councils, but are rather done individually by each company at the corporate level. As a result, government coordination with industry through the sector Coordinating Councils, while convenient and useful in many respects, does not adequately reflect the complexity of issues industry actually faces in making the critical cyber security decisions that affect their government partners. For the public-private partnership to evolve toward maximum effectiveness, this complexity must be appreciated, meaning that the partnership must become meaningful to industry at the business plan level.

While such an arrangement may at first sound daunting, there is a rich and successful history of similar industry-government partnerships for non-cyber infrastructure enhancement. For example, a century ago the hot technologies were electricity and telephone networks. Originally, these services were provided by private companies who served only areas that met their economic self-interests, which meant redundant competitive services in high profit areas and little or no service to less financially attractive markets.

Policymakers realized that a great public service could be created by providing universal telephone and electric service, but that the natural economics were unlikely to achieve this goal. Instead they resolved the situation by creating a "social contract," wherein the government essentially guaranteed the private investment in telephones and electricity providers (thus turning them into public utilities) in return for the social good of universal service at affordable rates. In so doing, government created an enduring and successful partnership for infrastructure enhancement increasing the profits and operating margins of the private sector. Proposals modeled on this "social contract" theory for cyber security are described in *The Cyber Security Social Contract* and *The Cyber Security Social Contract 2.0*.[23]

Perspective Taking

One of the major causes of relational difficulty is when one partner assumes that the other will behave as they would, thus not only fail to appreciate their differences, but not going the next step to "walk a mile in his shoes." In human relationships, perspective taking (closely aligned with empathy) refers to the ability to see things from your partner's point of view. While both industry and government may also have aligned interests with respect to overall cyber security, there are other interests under consideration that lead to different perspectives and assessments of otherwise similar situations or circumstances.

Government's fundamental role under the U.S. Constitution is to provide for the common defense. Industry's role, backed by nearly a hundred years of case law, is to maximize shareholder value.[24, 25] A general consensus has emerged that the most effective path to cybersecurity is a risk-based approach that encompasses an assessment of threats, vulnerabilities, and consequences. However, government partners and industry players often assess risk differently, based on their differing missions and objectives.

Typically, private sector entities assess risk in terms of the economic consequences. Firms may, and often do, decide to allow for a certain amount of insecurity (e.g., pilfering) as a cost of doing business if the investment required to create a higher standard of security is not cost effective.

Government has an inherently lower tolerance for risk because of their higher calling for citizen defense and they are faced with multiple non-economic issues—including public perception and political considerations. Furthermore, compared to private industry, government has a greater ability to simply create funding should they desire to do so. Corporations, on the other hand, may well come to a different conclusion on the need for various cyber security investments.

For the partnership to endure and grow, an appreciation of these differing perspectives—born from different legally mandated responsibilities—must be reached. It may well be that government requires greater investment in cyber security to serve the national interest than a specific company requires for its corporate interest.

It may be unreasonable to assume that private companies will, or can, perennially make non-economically justified investments in cyber security. The government should compensate private entities for making investments that align with the government's perspective, such as the

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

social contract, rather than mandating that the shareholders subsidize the government function of providing for the common defense.

Flexibility

A natural extension of appreciating that relationships are complex and can be facilitated when the partners can take the perspective of the other is the notion that the ability to adapt, to be flexible, is a valuable skill.

In the context of the cyber security partnership, this translates into the appreciation that there is not a simple gold standard, or mandatory minimum standard of cyber security. The Internet is a network of networks operated for varying purposes in numerous cultures and operating with differing equipment.

Using existing mechanisms, the partnership will need to evolve a flexible set of standards which can be independently assessed for their varying degrees of effectiveness. With the creation of this "sliding scale" of effective standards practices and technologies, government will be able to offer varying incentives (procurement, liability, tax, insurance, streamlined regulation, etc.) in return for voluntary adoption of security measures. Enterprises might then elect to enhance their security because it appeals to their broad business interests rather than as a matter of regulatory compliance.

Conclusion

Just like any relationship, the public-private partnership is bound to encounter difficulties. However, it is impractical for one partner to attempt to seize control of the partnership and attempt to bend the other to its will. Instead, partners need to remain committed to the relationship and continue working on it by understanding the complexity of the situation, adapting where appropriate to their partner's perspective and evolving a flexible system of rewards and incentives to enhance the overall security of both industry and the government.

About the Author

Larry Clinton is President and CEO of the Internet Security Alliance (ISA). ISA represents major corporations from the Aviation, Banking, Communications, Defense, Education, Financial Services Insurance, Manufacturing, Technology and Security industries. ISA's mission is to

integrate advanced technology with economics and public policy to create a sustainable system of cyber security. Mr. Clinton is one of the clearest voices on cyber security and has been featured in mass media such as *USA Today*, *PBS News Hour*, *The Morning Show (CBS)*, *Fox News*, *CNN*, *C-SPAN*, and *CNBC*. He has also authored numerous professional journal articles on cyber security as well as being a past guest editor for the Cutter IT Journal. Mr. Clinton is regularly called upon to testify before both the U.S. House and Senate. In 2008, ISA published its Cyber Security Social Contract which is both the first and last source cited in the Executive Summary of President Obama's *Cyber Space Policy Review*, which also cited more than a dozen ISA white papers—far more than any other source.

References

1 Dennis C. Blair, testimony before the Senate Select Committee on Intelligence, 111th Congress, 1st Session, February 2, 2010.

2 Executive Office of the President, *The National Strategy to Secure Cyberspace*, February 2003.

3 *National Infrastructure Protection Plan*, 2006.

4 Executive Office of the President, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure* (Washington, DC: The White House, May 2009).

5 *National Infrastructure Protection Plan*, 2006 at 9.

6 Executive Office of the President, *Cyberspace Policy Review—Assuring a Trusted and Resilient Information and Communications Infrastructure*, May 2009.

7 Ibid.

8 George Herbert Mead, *Symbolic Interactionism Role Taking Role Making the Generalized Other*, 1934.

9 United States Government Accountability Office (GAO), *Critical Infrastructure Protection: Current Cyber Sector-Specific Planning Approach Needs Reassessment*, September 2009, 2.

10 Lewis, James, *Cybersecurity Two Years Later*, January 2011.

11 Ibid.

12 Staff Draft Combining S773 and S3480, 111th Congress, August 2010.

13 Em Griffin, *Communication, Communication, Communication: A First Look at Communication Theory* (New York, NY: McGraw Hill, 2009); see also: Herbert Blummer, *Symbolic Interaction* (Edgewood Cliffs, NJ: Prentice Hall, 1969).

14 Aerospace Industries Association Annual Conference, *Robert Bigman comments on Cyber Security*, Washington, D.C., October 2008.

https://scholarcommons.usf.edu/jss/vol4/iss2/7
DOI: http://dx.doi.org/10.5038/1944-0472.4.2.6

15 U.S. Senate, hearing before the Committee on Judiciary, Subcommittee on Terrorism and Homeland Security, *Testimony of Richard C. Schaffer, Jr. Information Assurance Director of the National Security Agency*, November 17, 2009, available at: *http://judiciary.senate.gov/pdf/11-17-09%20Schaeffer%20Testimony.pdf*.

16 PricewaterhouseCoopers, *The Global State of Information Security*, 2005.

17 Wade Baker et al., "2010 Data Breach Investigations Report," *Verizon*, 2010, available at: *http://tinyurl.com/26cqfj2 (www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf)*.

18 Remarks by President Obama at the White House on cybersecurity, July 14, 2010.

19 Jeff Brown, "Disrupting Attacker Command and Control Channels: A New Model for Information Sharing," in *The Cyber Security Social Contract:2.0* (Washington, D.C.: Internet Security Alliance, 2009).

20 Business Software Alliance, Center for Democracy & Technology, U.S. Chamber of Commerce, Internet Security Alliance, TechAmerica; *Improving our Nation's Cybersecurity through the Public-Private Partnership: A White Paper*, March 2011, available at: *http://www.isalliance.org*.

21 Hart R. P and Burks D, M., "Rhetorical Sensitivity and Social Interaction Speech Monogaphs," 1972, 39.

22 Appelgate J, "Constructs and Communication: A pragmatic Integration," in R Neimeyer and G Neimeyer eds. *Advances in Personal Construct Psychology*, 1990.

23 Internet Security Alliance, *The Cyber Security Social Contract:2.0*, December 2009; Internet Security Alliance, *The Cyber Security Social Contract: Policy Recommendations for the Obama Administration and 111th Congress*, 2008.

24 *Dodge v. Ford Motor Co.*, 170 N.W. 668 (Mich.1919).

25 *Carlton Investments v. TLC Beatrice International Holding, Inc.*, 1997 Del. Ch. LEXIS 86, 45 (ct. of Chancery, New Castle May 30, 1997).