

Journal of Homeland Security and Emergency Management

Volume 6, Issue 1

2009

Article 79

The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen

Richard J. Harknett*

James A. Stever†

*University of Cincinnati, richard.harknett@uc.edu

†University of Cincinnati, steverja@fuse.net

The Cybersecurity Triad: Government, Private Sector Partners, and the Engaged Cybersecurity Citizen*

Richard J. Harknett and James A. Stever

Abstract

In May 2009, the Obama administration released its, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*, which it expected would lay the groundwork for a new national cybersecurity strategy. Staking out separate policy development space, Congressional leaders began hearings and introduced legislation. The most significant – the Cybersecurity Act of 2009 – proposed major changes in current federal government approaches. The common starting point of all of these reform efforts is that current federal organization and current national cybersecurity policy is inadequate for the task of securing cyberspace.

This article analyzes past federal reorganization efforts in response to the last technological revolution with serious national security implications – nuclear technology – and the more recent response to homeland security. While much of the current cybersecurity debate leans toward radical reforming, we counsel an incremental approach to reorganization that builds on the hard work of the last decade combined with a genuine reconceptualization of the threat solution set. Borrowing from the language of the nuclear era, we call for cybersecurity to rest on a balanced triad of intergovernmental relations, private corporate involvement, and active cyber citizenship as a resilient model that can manage this new and challenging security environment. In particular, we introduce the third leg as a critical new concept that has been absent from standard policy debate. The road to cybersecurity is destined to be long, circuitous, and difficult. Extensive negotiations between federal, state, local, and private sector leaders loom. No truly significant federal policy reform can be achieved without considering the intergovernmental policy dimensions combined with the overall threat perception driving those reforms. Success will remain elusive if government to private business relations do not improve and much will be undermined if the general public remains inactive in contributing to national cybersecurity.

KEYWORDS: Obama cyber policy review, cybersecurity, intergovernmental relations

*The authors wish to thank the Charles Phelps Taft Memorial Fund and Research Center at the University of Cincinnati for its financial support, which has allowed open access publication of this article.

INTRODUCTION

Cyberspace – the totality of computer networks and related programmable electronic devices and their integrated communication – is a vital dimension of the 21st Century. This new and pervasive technology supports daily life in the United States, is a realm of tremendous economic activity, and provides the infrastructure for electricity, transportation, food production, communication, etc. Unfortunately, the functionalities provided through cyberspace are very vulnerable, and the collapse of interrelated networks could result in catastrophic outcomes. Closing these vulnerabilities and managing threats to cyber-infrastructure is a vital national security interest of the United States.

In 2009, the US Congress and the Obama Administration reviewed existing cybersecurity efforts and considered a range of options from incremental modification to wholesale reinvention. This article counsels an incremental approach. Much of the adaptation to cyberspace that has been accelerating over the past fifteen years need not be jettisoned. However, what is required is a new conceptualization of how federal, state, and local governments should be involved in this endeavor. This new conceptualization will make it easier to subsequently involve both the private sector and the general public. Despite immediate vulnerabilities, we must recognize that the complexity of the challenge will require many years and many refinements before the objective of a stable and secure cyberspace will be achieved.

In May 2009, the Obama administration released its, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* that it expected would lay the groundwork for a national cybersecurity strategy.¹ Staking out separate policy development space, Congressional leaders began hearings and introduced legislation.² The most significant – the Cybersecurity Act of 2009 – proposes major changes in current federal government approaches including mandating the transfer of responsibility for cybersecurity from the Department of Homeland Security (DHS) to the White House Executive Office and involvement of the Department of Commerce. Much of this reassessment activity, including critical reports from the Government Accountability Office (Powner, 2009) and the Commission on Cyber Security for the 44th Presidency (CSIS, 2008), springs from a sense that DHS has failed to meet its responsibility to secure the nation's computer networks.

¹. The *Cyber Policy Review* was essentially an overview of a plan to write a new security strategy under White House direction. For full report please see, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

². Senator Joseph Lieberman, for example, introduced the Critical Electric Infrastructure Protection Act of 2009 with specific focus on cyber threats. (Lieberman, 2009).

In a convulsive act of reorganization in response to the attacks of September 11, 2001, Congress created DHS through the Homeland Security Act of 2002. Securing cyberspace was included among its many responsibilities. It is important to recognize that the United States is only eight short years into a remarkable re-organization of overall domestic intergovernmental relations as they relate to national and homeland security. In seeking to address deficiencies in the area of cybersecurity, we must take care to assess whether the fundamentals contained in the original Homeland Security Act of 2002 need to be cast aside or whether refinement of the institutional organizations and processes under development since 2002 and earlier will produce more sustainable security policy outcomes.

This article makes the skeptical argument that even if responsibility for cybersecurity is successfully moved to the Executive Office of the Presidency, much more reorganization and governance changes will be required to implement cybersecurity policy effectively throughout the American federal system. The reorganization required to achieve cybersecurity is strategic and adaptive in nature. Simple centralization will not produce cybersecurity. The following parameters should guide this reorganization.

First, is the essential recognition that cyber threats pose a national security challenge. Cyber threats are more serious than a nuisance or crime. Second, intergovernmental management problems are inevitably a part of the cyber challenge. State and local governments are destined to be key actors in meeting future cyber threats. Third, involving state and local governments will facilitate partnerships with the private sector corporations that operate critical cyber infrastructure. Finally, the general population, the end users of computer technology, must be mobilized and involved in any successful cybersecurity

Securing cyberspace is iterative rather than linear and can be understood best as resting on three legs of core institutional and process relationships – a cybersecurity triad. The first leg is intergovernmental, which is defined both in terms of federal interagency relationships and in the layers of relationships between the federal government and state and local governments. The second leg is public-private in terms of government to private business and critical infrastructure relations. The final leg is integrating the general population into this endeavor. Current analysts tend to go little beyond superficial considerations of citizenry privacy rights versus government cyber regulation. While privacy is a significant and contentious issue, the focus on ‘Big Brother’ has crowded out the more important issue of the general population’s responsibility to government. A culture of cybersecurity citizenship must be developed that encourages the American population writ large to change its behavior and take more responsibility in ensuring cybersecurity.

The following two sections draw out these observations through review of past major reorganizations and some analogous reasoning from the nuclear era.

LESSONS FROM HOMELAND SECURITY

THE FIRST LEG OF THE CYBERSECURITY TRIAD: INTERGOVERNMENTAL RELATIONS

The Department of Homeland Security (DHS) provides a cornucopia of information about how intergovernmental policy implementation actually occurs. The Congress created this agency in 2002 by placing twenty-two existing agencies or pieces of agencies under the DHS umbrella. Hence, the initial task was integrating these components into a coherent homeland security mission as well as coordinating the new DHS mission with other executive agencies. For example, DHS acquired the Federal Emergency Management Agency (FEMA), and during the first two years of its existence, the agency utilized the pre-existing FEMA *Federal Response Plan* published in 1992 as its blueprint for managing catastrophic disasters. This plan reads as little more than a codified set of agreements among federal agencies on the protocol to be followed during natural disasters.

In July, 2002, the Bush White House published its *National Strategy for Homeland Security*. The passage below from the executive summary suggests that the president was looking ahead in anticipation of looming intergovernmental issues.

American democracy is rooted in the precepts of federalism—a system of government in which our state governments share power with federal institutions. Our structure of overlapping federal, state, and local governance—our country has more than 87,000 different jurisdictions—provides unique opportunity and challenges for our homeland security efforts. (Homeland Security, 2002, vii)

However, DHS did not signal how it intended to tackle the thorny problems associated with implementing its policies at the state and local level until December, 2004 when it issued its first major document, *The National Response Plan* (NRP).

The DHS delay in issuing the *NRP* is understandable. FEMA's *Federal Response Plan* contained little intergovernmental policy guidance. Moreover, the Congress gave DHS a significantly greater domestic security mission than it had given to FEMA nearly two decades previous: i.e., management of

catastrophic disasters as well as mitigation, preparedness, and response to terrorism. Prudently, DHS moved slowly to implement its new domestic security policies throughout the federal system.

Intergovernmentally, the *NRP* represents an advance beyond FEMA's *Federal Response Plan*; however, it was only an incremental advance. Section III of the 62-page basic document briefly describes and specifies in seven pages the new domestic security roles and responsibilities of Governors, local officials, tribal officials, non-profit agencies and private sector institutions. These seven pages were hortatory in the sense that they provided guidance to subnational and private sector institutions anxious to cooperate, but DHS had few enforcement tools at its disposal to compel compliance. To encourage state and local cooperation, DHS could only use the same tool other domestic policy agencies rely upon -- federal grants.³

The successor document to the *NRP* is the *National Response Framework* issued in January, 2008. Intergovernmentally, this document is, again, an incremental advance. This new ninety-eight page guidance devotes two sections to state, local, and private sector roles totaling only 17 pages. DHS critics can point out that the agency's intergovernmental pace has been slow. Yet, the 17 pages of this 2008 document devoted to intergovernmental domestic security policy has been preceded by countless hours of consultation with state and local leaders and with the private sector. These consultations developed the necessary linkages for further policy refinement and implementation, and were essential because DHS has minimal constitutional powers at its disposal to command these subnational entities to comply with its directives.

DHS chose to address cybersecurity issues within the context of its *National Infrastructure Protection Plan* introduced in 2006, then redrafted in 2009. DHS identified seventeen infrastructure sectors ranging from energy to banking and finance. The plan's intergovernmental approach has been to identify a federal agency responsible for a specific sector, then make that agency responsible for chairing a Government Coordinating Council made up of federal, state, and local representatives knowledgeable about critical infrastructure within the specific sector. These coordinating councils were then encouraged to interact with their counterparts in the private sector that DHS had recruited into Sector Coordinating Councils. The hope was that the interaction of the Government

³. President Bush issued Homeland Security Presidential Directive # 8 in December, 2003 and announced the eventual creation of a "National Preparedness Standard" that would hold state and local governments accountable. However, the standard itself is inevitably general. DHS has created 36 "Target Capabilities" and a Universal Task List to further guide state and local preparation. The jury is still out on the effectiveness of these accountability measures.

Coordinating Councils and the Sector Coordinating Councils would produce infrastructure policy recommendations upon which DHS could act.

DHS chose not to treat the internet as a separate and distinct infrastructure. Rather, it specified that cybersecurity was a “dimension” that ran through each of the seventeen infrastructure sectors. It is unclear where the Obama administration will move on this critical organizational and conceptual issue. In their *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* the initial step outlined is to bring coordinating functions into the White House. This move elevates attention to the issue of cybersecurity and will encourage interagency activity as the federal bureaucracy responds to presidential-level initiative and concern. These Obama initiatives need not displace prior DHS cyber policy, however, particularly the DHS decision treating cybersecurity as a dimension across critical infrastructures sectors, rather than a realm to itself.

The DHS intergovernmental strategy for cybersecurity is open to improvement. The agency resorted to the language of partnership hoping that the cooperative approach would energize relationships between Government Coordinating Councils and their private counterparts in the Sector Coordinating Councils. The level of cooperation between the councils in the various infrastructure sectors has been uneven. Moreover, each sector has considerable latitude to craft its own cybersecurity strategy. DHS can legitimately argue that this latitude is appropriate given the fact that the cybersecurity requirements of the agricultural sector will vary from those required of the military or the banking sectors. Whether the White House Office of Cybersecurity would allow these differences to exist organizationally has yet to be determined, but such a structure should remain under consideration for refinement, rather than all-out replacement.

Additionally, the 2009 *Cyberspace Policy Review* calls on the cyber coordinator to be the center of policy development and dual-hats the coordinator with seats on both the National Security Council and the National Economic Council. In the absence of direct presidential line authority, the open question remains over whether the cyber coordinator will be able to influence both councils or will be pulled between their competing perspectives. The coordinator will have some mild budgetary influence by virtue of some access to the Office of Management and Budget (OMB) priority process. However, assuming this OMB link will cause agencies to emphasize cybersecurity in their budget priorities without substantial new resources proffered is wishful thinking.

A key point to consider is the difference between centralization and coordination. While the media has defaulted to the term “cyber-czar,” the *Cyberspace Policy Review* and the president’s announcement of the position avoided use of the term and specifically referred to the position as a coordinator. Such semantics and titling are important if they rest on the more advisable

presumption that cybersecurity will not be enhanced through centralized control, but rather through the resiliency that a coordinated cyber-triad can produce.⁴

The 2009 *Cyberspace Policy Review* provides only initial thinking on the development of state and local intergovernmental relations. The review aspires to achieve improved state and local cooperation/compliance. It notes that one obstacle in these jurisdictions has been the lack of prioritization and ownership of cybersecurity because different aspects of the problem are handled by Chief Information Officers, Chief Information Security Officers, and State Homeland Security Advisors. Consolidation of efforts at the State level around state and local cyber coordinators would help, but such appointments likely will receive scant attention if not backed with budgetary incentives or regulatory sanctions. White House linkage, by itself, is unlikely to alter and shape cybersecurity practices in State and local jurisdictions unless priorities change, which is unlikely without real budgetary incentives.

The organizational aspects of interagency and intergovernmental processes are a key element of an effective first leg of the cyber-triad, but the solution set is not to be found solely in organizational charts. Critical is the yet-to-be-fully-established threat prioritization backed through budgetary and regulatory mechanisms that shape the actual information flow through public and private sector cyber networks.⁵

THE SECOND LEG OF THE CYBERSECURITY TRIAD: PUBLIC-PRIVATE RELATIONS

The 2009 *Cybersecurity Policy Review* offered the requisite support for the second leg of our cyber-triad – public-private relations – but remained flexibly ambiguous about how those relationships can be improved. As the Obama administration moves forward in establishing a new national cybersecurity strategy, it should follow the same effective principles regarding intergovernmental relations – refinement of existing organizations and processes, rather than radical reform.

⁴. One should note that the track record of presidential coordinators is mixed. Ashton B. Carter, for example argues that White House “czars” are seldom effective. “After the czar is thus overridden a few times, lower-level bureaucrats conclude that the czar’s directives can be ignored. As the Washington saying about czars goes, the barons ignore them, and eventually the peasants kill them.” (Carter, 12).

⁵. In 2007 the Bush Administration launched the Comprehensive National Cybersecurity Initiative (CNCI), which is meant to achieve this prioritization within executive branch agencies. The CNCI remains classified and the scant reference to it in the 2009 *Cybersecurity Policy Review* suggests that it is making progress that can be built upon.

The scale of trust and confidence-building measures and the actual confidence gained over the past 11 years since Presidential Decision Directive 63 (PDD-63) was signed in 1998 calling for information sharing and coordination across the nation's critical infrastructures can not be underestimated. The public-private cyber relationship is an uneasy complicated context of unaligned priorities that parallel a general agreement that cyber vulnerabilities are serious. The 2009 *Cybersecurity Policy Review* does note that many groups and forum have been established to manage the relationship and suggests that there is a downside to the proliferation of efforts in the form of inefficiencies and ill-defined roles. While true, there are also real benefits that have been accrued collectively over the past decade and some inefficiency must exist due to the nature of the challenge. In recognizing this and attempting to find improvement, again, the default should be toward better coordination rather than centralization. For example, private sector-based Information Sharing and Advisory Councils (ISACs) exist across fourteen critical national infrastructures (such as transportation, water safety, electricity) and represent a wealth of experience and capacity.(ISAC, 2009) Similarly, constructs such as the Critical Infrastructure Protection Initiative's Government Coordinating Councils and their private counterparts in the Sector Coordinating Councils require innovative improvement, but represent existing structures of value. Another example is the FBI's InfraGard partnership, which facilitates information-sharing at the local level with the private sector through FBI regional offices. While more focus must be directed toward reducing unnecessary bureaucratic overlap with DHS, enabling area competencies such as FBI-field offices and cybercrime should be leveraged to engage private partners at the local level. Greater coordination, rather than centralization, should be the first step of intergovernmental and public-private relations reform.

Improving the relationship between existing clusters of cyber expertise and their lead government agencies should be a major priority within the emerging debate over cybersecurity strategy. The dual-hatted nature of the White House Cyber Coordinator, with a place at both the NSC and the NEC, must be leveraged to create greater synergy of perspective over the security of economic activity and the economics of security. There must be emphasis placed on creating a new regulatory model not based on 19th and 20th century dynamics, but rather one that undergirds the synergy between national cybersecurity and private sector activity. Market-based solutions alone will not lead cumulatively to a more secure environment. Private sector efforts must be coupled with federal regulatory parameters to produce the mutually beneficial outcome of a more secure cyberspace.⁶

⁶. The private sector has significant incentive to increase security to reduce fraud. However, increased security has often taken a backseat to customer convenience. A University Michigan

LESSONS FROM THE LAST TECHNOLOGICAL REVOLUTION

PREVIOUS INCREMENTAL SECURITY SUCCESSES

This is not the first time that the United States has faced significant technological developments impacting national security at a moment of geo-political shifts. In the late 1940s, the United States emerged as the leading economic and military country in the aftermath of the Second World War and quickly had to adjust its domestic intergovernmental structures to grapple with that status. Such a re-organization was also spurred through the recognition that the uniqueness of the atomic bomb required creative civil-military arrangements. The National Security Act of 1947 began to address the United States' status as world power.⁷ It created the National Security Council (within the Executive Branch to coordinate across key agencies and enhance strategic planning), the Central Intelligence Agency, and the Defense Department, along with the Air Force as a stand alone military service. The Act established congressional oversight functions as well as preliminary conditions of intelligence reporting and classification. What is important to extract from the history of the 1947 Act was that it was amended only two years later to enhance the Secretary of Defense's power and has been consistently refined since.⁸ The National Security Act of 1947 also laid the foundation for subsequent core institutional arrangements that dealt with the many facets of the nuclear condition: i.e., how to manage the production, deployment, and possible use of nuclear weapons; how to prepare for the eventual possession by other states; and how to deal with the dual-use potential of civilian nuclear energy production.

In a similar sequence, the Atomic Energy Commission was created in 1946 to directly manage the nuclear issue and put in place the core notion of government civilian control over both military and potential economic uses. The Atomic Energy Act Amendments of 1954 set the conditions for private production of civilian energy use and for federal government regulation, which stayed in place for twenty years until in 1974 when the regulatory and promotional/production functions of the AEC were split with a major

study of 214 financial websites found that 76% had at least one design flaw that exposed customers to unnecessary security risks. If one assumes that financial websites represent some of the better cases of secure cyberspace, this finding is troubling. (Falk, 2008)

⁷. Full Text of National Security Act of 1947, http://www.intelligence.gov/0-atseact_1947.shtml

⁸. Similarly, the Homeland Security Act of 2002 was refined a year later through Homeland Security Presidential Directive 7, which designated the Secretary of DHS as coordinator of critical infrastructure protection. In the aftermath of Hurricane Katrina in 2006, Congress amended the HAS of 2002 to reorganize DHS, establishing an Office for Cybersecurity and Communications under a new Assistant Secretary. (White House, C10-11).

reorganization (creation of the Nuclear Regulatory Agency and eventually the Department of Energy).

The notion that the 1947 National Security Act and the 1946 Atomic Energy Act could be revised, rather than discarded, forty years and thirty years, respectively should provide those examining the Homeland Security Act of 2002 some pause on radical revisions so early in the implementation stage. The real guts of intergovernmental relations are, not so much the organization chart, but the intricate interaction of real expertise across different layers of government. In the absence of real failure, incremental refinement should remain the default assumption of institutional change efforts, rather than a preference for radical restructuring.

THE THIRD LEG OF THE CYBERSECURITY TRIAD: CYBERSECURITY CITIZENSHIP

At first glance, cyber technology resembles nuclear technology in that both can be used for peaceful and for hostile purposes. Though the dark side of nuclear technology prevailed initially, President Eisenhower's "Atoms for Peace" speech to the United Nations in 1953 attempted to convince the world that nuclear power could be harnessed to improve the condition of all mankind. However, cyber technology needs no such positive bolstering. Computer technology has been readily embraced by the business community, by children in elementary schools, and has become as familiar and indispensable as the television set within the home.

What has garnered less attention in discussions of cybersecurity challenges is the essential relationship between the government and the general population. While the threat from nuclear weapons was rather obvious to most in the 1950s, the notion of cyber threats as more than nuisance (viruses/spam) or crime (identity theft) is not widely appreciated.⁹ Moreover, the general populations' complicity in weakening national cybersecurity goes unrecognized. The emergence of botnets as a serious cyber threat is a key case in point as these represent clusters of compromised personal computers that can be connected to produce major increases in computing power. The July 2009 distributed-denial-of-service attacks on American and South Korean government sites may have involved 50,000 compromised computers. Vulnerable personal computers create national vulnerability.

⁹. The National Cybersecurity Alliance found in its October 2008 survey that while anti-virus software use was up significantly, only 58% of users indicated that they had active firewalls and 42% used anti-spam filters. Since the latter represents a major delivery approach for viruses, low use of protective software creates a continuing vulnerability.

Sensitivity of the United States' citizenry to nuclear technology's dark side explains the initial widespread popular support for the Civil Defense Act of 1950. This act funded the construction and supplying of bomb shelters, planning for evacuation of large population centers, and training in civil defense procedures. Eventually, support for civil defense waned as skeptics questioned the effectiveness of such measures. By 1955, the state of New York resorted to the stick—threatening to impose a \$500 fine on anyone failing to seek shelter during a civil defense drill.

In retrospect, the United States did not find it necessary to fully integrate its state and local governments, much less the private sector into a civil defense policy to manage the nuclear threat. It soon became clear that thermonuclear weapons possessed at a certain level could assure the destruction of society in general. While civil defense planning continued, it was supplanted with a military strategy and command and control system predicated on assuring the destruction of the Soviet Union even after absorbing a surprise attack (creation of the nuclear triad to provide assured second strike capacity). The strategy of nuclear deterrence prevailed, and notions of civilian defense were quietly set aside. In essence, the overwhelming lethal power of nuclear weapons obviated the need for the federal government to cajole or force state and local governments, private sector institutions, and the public to submit and participate in a civilian defense effort. Concerns that were raised in the 1960s over the domestic militarization of the United States dissipated.

The cyber threat is different. The ubiquity of computer technology throughout the civilian population will require full societal engagement if the national objective is a secure cyberspace. As the digital environment grows in scale and scope, so too will the need for a cyber civic culture to emerge to manage it. Ironically, because the citizenry is less conscious of the cyber than the nuclear threat (as national security threat), a much greater degree of civic mobilization and understanding will be required to face this 21st Century challenge.

Thus, while effective intergovernmental relations and private sector coordination are essential to deal with cybersecurity, the final element and perhaps most significant departure from current policy must be a concerted education effort that establishes a relationship between the general public and cybersecurity. Cybersecurity oriented intergovernmental relations and public-corporate coordination will be difficult to perfect, but advances in those areas will be impossible if cyberspace continues to be conceived primarily as a private concern rather than a public good.

Section 10 of Senator Rockefeller and Snowe's draft 2009 legislation calls for a cybersecurity awareness campaign—though they provide little guidance for such an effort. The 2009 *Cybersecurity Policy Review* devotes a few lines that call for an education campaign that “should focus on public messages to promote

responsible use of the Internet and awareness of fraud, identity theft, cyber predators, and cyber ethics.” (White House, 14) Cybersecurity citizenship should not be an afterthought, but must be a lead element of any reorganization effort. Cybersecurity depends not only on reorganizing agencies, but reorienting civic culture. The general population must be engaged as active security providers, not simply beneficiaries of security policy, because their practices often create the threats to which government must respond. Any awareness campaign that remains seated in only self-interest (if you do not protect yourselves bad things will happen to you) will not establish this critical third leg of the cybersecurity triad. A national public interest construct must be created that convinces the citizenry that cybersecurity is a civic duty. This campaign would bear some similarity to the Civil Defense efforts of the 1950s.

In response to the nuclear threat, the Truman administration created through Executive Order the Federal Civil Defense Administration. Congress gave this agency responsibility for creating civil defense programs that local and state governments could adopt. Military and foreign policy were directed, of course, to mitigate the nuclear threat, while the main purpose of civil defense efforts was to improve population survival in the aftermath of a nuclear attack. An extensive information program preached the need for preparedness and self-reliance in the immediate aftermath of an attack. The government supported public fall-out shelters and, until 1961, city-scale size evacuation drills. Recent efforts concerning response to terrorist attacks have built upon this civil defense legacy, which transitioned in the later part of the Cold War to a more fully-integrated emergency management system.

However, beyond the above similarity, cybersecurity citizenship obviously must develop in a different context than 1950s Civil Defense. Cyber technology is pervasive throughout society. The internet transforms individual computer users into actors that participate in an interdependent, connected cyber system. In contrast to nuclear technology, those who utilize cyber technology pay minimal opportunity costs. They are not required to register their computer with government security agencies. They receive no standardized training, and they presently possess the constitutional right to contract with whomever they wish to repair, replace, or improve their computer. Most users remain unaware that not only is their computer data vulnerable, but that their insecure access to cyberspace can be exploited by others turning them into unwitting agents of coordinated cyber threats (both criminal and disruptive attacks).

Thus, the key reorientation of any cyber awareness plan must hinge on the notion of active participation in enhancing national security as a civic duty.¹⁰

¹⁰. The National Cyber Security Alliance and its related government partners have developed an awareness campaign on the notion of shared responsibility. Our notion of a civic duty elevates

While civil defense is premised on population survival after an attack, cyber civil security assumes that every citizen is an active participant in enhancing security in cyberspace. Cybersecurity must become a national civic responsibility. Practicing safe computer practices regarding passwords, security software, downloading protocols all contribute to mitigating the weakest links across cyberspace. The notion of cyber civic security is that the general population must take responsibility for actively (and daily) providing for national cybersecurity (not just individual cybersecurity). Establishing a national ethos about cybersecurity responsibility will be as an enormous a task as federal reorganization, because such a civic ethos must displace established practice and views. For example, hacking by teenage pranksters is treated as a nuisance, not as breaking and entering or as a serious security threat with appropriate punishment. A more secure cyberspace will not occur if the public remains indifferent to the exigencies of cybersecurity. Here the government and the private sector have a mutual interest. An integrated campaign not simply from the government, but including private corporate effort is possible. A small fraction of the digital fraud that the business community must write-off their profit margins each year spent on a public awareness campaign could produce real dividends. In the end, achieving cybersecurity will involve not only technical advances and effective organizational responses, but behavioral changes by end users. While there are limits to its effectiveness, federal and private efforts at socialization and supervision of end users is a necessary element of a comprehensive national cybersecurity strategy. In particular, dedicated effort must be built into our K-12 education curriculum so that secure computing becomes the foundational base when learning to read, write, and work in the digital age.¹¹

CONCLUSION

The road to cybersecurity is destined to be long, circuitous, and difficult. Extensive negotiations between federal, state, local, and private sector leaders loom. No truly significant federal policy reform can be achieved without considering the intergovernmental policy dimensions combined with the overall

cybersecurity even further and places the emphasis on the individual producing a collective outcome regardless of what the government does. Secure home computing does not require a shared partnering with government, it requires individual duty. This is more than mere semantics. The NCSA's efforts are very important and should be the basis for a prioritization that comes through the Obama Administration's national cybersecurity strategy. The third leg of the cybersecurity triad must be bolstered immediately and sustained for the long-term. For efforts to build upon see, <http://staysafeonline.org> ; OnguardOnline.gov ; DHS.gov/cyber

¹¹. A 2008 survey indicated K-12 teachers felt they lacked expertise, resources, and dedicated classroom time to competently teach cyberethics, cybersafety and cybersecurity. (NCSA, 2008)

threat perception driving those reforms. Success will remain elusive if government to private business relations do not improve and much will be undermined if the general public remains inactive in contributing to national security.

However, an incremental approach to reorganization that builds on the hard work of the last decade combined with a genuine reconceptualization of the problem can lead to success. A balanced triad of intergovernmental relations, private corporate involvement, and active cyber citizenship is a resilient model that can manage this new and challenging security environment.

REFERENCES

Carter, Ashton B (Winter 2001/2) "The Architecture of Government in the Face of Terrorism," *International Security*, Vol 26, No. 3.

CSIS Commission on Cybersecurity for the 44th Presidency (December 2008) *Securing Cyberspace for the 44th Presidency*, Washington, DC: Center for Strategic and International Studies.

Homeland Security, Office of (2002) *National Strategy for Homeland Security*, (Washington, DC, Government Printing Office).

Information Sharing and Advisory Council (January 2009) "The Role of ISACs in Private/Public Sector Critical Infrastructure Protection,"
http://www.isaccouncil.org/whitepapers/files/ISAC_Role_in_CIP.pdf

Lieberman, Joseph (2009) *Critical Electric Infrastructure Protection Act of 2009*. 111th Congress 1st session, S.946.

National Cyber Security Alliance (October 2008) *National Cyberethics, Cybersafety, Cybersecurity Baseline Study*
<http://staysafeonline.mediaroom.com/index.php?s=67&item=44>

National Cyber Security Alliance/Symantec (October 2008) *Home User Study*,
<http://staysafeonline.mediaroom.com/index.php?s=67&item=46>

National Security Act (1947),
http://www.intelligence.gov/0-natsecact_1947.shtml

Powner, David (2009) *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, Testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives, (March 10, 2009), GAO-09-432T

White House (May 2009) *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*
www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf