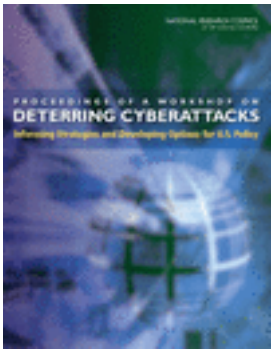

Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy

Committee on Deterring Cyberattacks: Informing Strategies and Developing Options; National Research Council

ISBN: 0-309-16086-3, 400 pages, 8 1/2 x 11, (2010)

The Organization of the United States Government and Private Sector for Achieving Cyber Deterrence

Paul Rosenzweig*
Red Branch Consulting

INTRODUCTION

A few years ago, the Central Intelligence Agency (CIA) working cooperatively with Saudi Arabia set up a "honey pot" website[1] to attract jihadi sympathizers. By all reports the website served as a useful intelligence gathering tool, giving the unseen CIA and Saudi observers insights into the activities and interests of the terrorists who frequented the site. By 2008, however, it had become apparent that some were using the website to make operational plans to infiltrate jihadists into Iraq where they would join the insurgency, potentially threatening the lives of American troops. The National Security Council (NSC) convened a group of representatives from the Department of Defense (DoD), CIA, Department of Justice (DOJ), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) to consider the matter. Eventually, over the CIA's objections, a DoD team from Joint Functional Component Command–Network Warfare (JFCC-NW) "took down" the website. Its actions caused collateral effects as far away as Germany, and disappointed our Saudi collaborators.[2]

The incident illuminates a host of definitional and policy issues and challenges in the cyber realm, many of which are considered in companion pieces for this study. But equally clear from this anecdote are the challenges we face from the lack of any effective, purpose-built, standing organizations or processes within the U.S. government for developing policy or making decisions about cyber attacks and cyber defense. Rather, as this particular event makes clear, critical decisions that may set precedent are frequently made in an ad hoc manner often without the benefit of either the time or inclination for a broader and comprehensive consideration of the policy implications of the decisions.

---

*Principal, Red Branch Consulting, PLLC, and Professorial Lecturer in Law, George Washington University School of Law. The author expresses his thanks to Nicholas Rueter, a J.D./M.A. candidate at Duke University, for his able research assistance. I am indebted to the participants in the NAS workshop, the anonymous reviewers of this paper, and particularly to the members of the panel, for their thoughtful review and comments which have improved this paper. The remaining errors are, of course, my own.

[1]A "honey pot" is a website that is designed with features intended to lure and entice potential visitors, much as honey attracts bees, or Winnie the Pooh.

[2]The details of this event were disclosed in Ellen Nakashima, Dismantling of Saudi-CIA Web site illustrates need for clearer cyberwar policies, Wash. Post at A01 (March 19, 2010) [available at http://www.washingtonpost.com/wp-dyn/content/article/2010/03/18/AR2010031805464.html].

The organizational deficit is two-fold: It is, first and foremost, a lack of structures for the *making* of a comprehensive policy and a lack of organizational cohesiveness in driving solutions forward in a way that includes all relevant stakeholders. It is, secondarily, a lack of adequate structures for *implementing* the policy decisions that have been made and for auditing our success (or failure) in doing so. This organizational deficit is not for a lack of effort. For more than 10 years, various Executive boards, agencies and working groups have struggled to create a cohesive framework for cyber decision-making.

Yet, today, most observers would agree that the U.S. has yet to develop a stable solution. As two well-regarded observers recently noted:

> [W]e also developed on an *ad hoc* basis over the last two decades various organizational structures in response to the cyber threat. Yet those infrastructure protection boards and cyber commissions typically lacked leadership, had no real authority, and were often made up of individuals who did not have combined expertise in national security, cyber security, policy, and law.
>
> Meanwhile, the private sector, owners of most of our critical cyber infrastructure, pursued an unstructured response to the threats, relying in the first instance on government systems for cyber security.[3]

A number of legitimate reasons explain why we have yet to develop these structures and processes. There are, first, several unique challenges inherent in deterring or preventing cyber attacks. These include the well-known attribution problem, the dependence of the civilian economy and military capability on information technology, and the difficulty in distinguishing between attack and exploitation. More prosaically, despite the proliferation of boards and commissions we simply have not paid enough sustained attention to the problem: organizational structures for the United States government to support our cyber deterrence activities have developed organically, over the past 20 years, through episodic and often reactive attention, rather than the product of a concerted policy-making process.

Then, too, by virtue of the nature of the cyber intrusions we have experienced, our organizational efforts have focused systematically on defensive measures rather than offensive ones. As a consequence, though our organizational structures for cyber defense are incomplete and lack coherence, with gaps and overlaps in responsibility and authority that have yet to be resolved, our structures for controlling attack/response mechanisms are even more immature and have yet to evolve to permit consideration of a "whole of government response" that would bring to bear all aspects of government power.

The lack of coherence is magnified because existing structures tend to conflate two distinct operational functions—those of policy decision-making and those of implementation. The function of setting deterrence policy and deciding a course of action will typically rest with governmental authorities. However, in the cyber domain (unlike, say, the nuclear domain), aspects of the implementation of those decisions will affect private sector actors who deploy their own defensive mechanisms and whose networks may be used to deliver a cyber response. The complex interaction between civilian, governmental, and military organizational structures for both offensive and defensive operations requires simplification.

This paper begins with a review of the history of existing American structures and processes within the Executive branch and examines the role of non-executive structures in the Legislative and Judicial branches of government. From this background the paper proceeds to a consideration of several particularly challenging questions relating to cyber deterrence policy and organization. This, in turn, allows for the development of recommendations for the improvement of the current structures.

I. A BRIEF INTERLUDE—A TAXONOMY OF DETERRENCE STRUCTURES

To some degree, a paper considering questions relating to the organization of the U.S. government's cyber deterrence response is premature. The organizational structures and procedures that the United States adopts to implement a policy of cyber deterrence should, optimally, be designed to implement the chosen underlying policy of deterrence itself. Form ought, ideally, to follow function, and in the absence of a clearly defined policy, defining a structure to implement a policy is hazardous, at best, and quite possibly counter-productive.

[3]William Banks & Elizabeth Rindskopf-Parker, Introduction, 4 J. Nat'l Sec. L. & Plcy. 1, 3 (2010).

Nonetheless, certain preliminary thoughts about organizational structures can be offered. But doing so requires the development of a taxonomy of deterrence, since in the cyber domain (as much, if not more so as in the physical world) our deterrence efforts will operate along several different tracks.

Broadly speaking traditional deterrence strategies are implemented through policies of denial and punishment.[4] In the context of the cyber domain, denial activities will involve a multifaceted approach that includes significant civilian participation. Punishment activities may well involve non-cyber responses that incorporate non-military (and possibly traditional kinetic military) actions. As a result, our cyber deterrence structures will need to be broad and wide ranging, and will likely vary depending upon which function the structures seek to support.

To that end, it is useful (or, at least, this author finds it useful) to identify certain subcategories of potential cyber deterrence activities for purposes of assessing the utility of current structures and processes. Within the area of denial, one can identify at least three distinct types of activity:

- *Cyber defense*—Classic activities of cybersecurity involving the detection and prevention of cyber intrusions or attacks.
- *Cyber resilience*—Activities relating to the strengthening of cyber networks so that even successful attacks have only limited effect because of redundancy and repair capacity built into the system.
- *Cyber systems assurance*—Activities relating to providing assurance that the cyber systems in use are not subject to foreign penetration or control.

Likewise, the area of punishment will, conceptually, involve at least two reasonably distinct activities that might require distinct structures:

- *Cyber attack*—Activities relating to a response to a cyber attack involving retaliatory (or preemptive) cyber action.
- *Non-cyber response*—Activities in response to a cyber attack not involving a cyber response (whether kinetic military acts or non-military acts).

And, finally, overarching all of these structures there exists a need for strategic-level structures that enable the *cyber coordination* of these various activities.

Not all of the structures that one can conceive of taxonomically have found a real-world analog within the federal government (or the private sector). To the contrary, while some (like cyber resilience structures) have a relatively long history (in cyber terms), others (like those relating to cyber assurance) are almost non-existent. In this section, we examine the existing federal organizational structures and processes and how they came to be.

A. Cyber Defense and Cyber Resilience to Protect Critical Infrastructure

Though conceptually distinct, the U.S. government has treated cyber defense and resilience functions as interrelated, and developed structures that seek to address both aspects of deterrence/denial through a single set of mechanisms.

Early Efforts

President Clinton made the first significant U.S. effort to address cyber defense and resilience issues with the issuance of Presidential Decision Directive (PDD)-63 in May 1998.[5] The directive noted the potential vulnerability of American infrastructure (ranging from transportation to water systems) and set forth a process for the development of an infrastructure assurance plan to protect critical assets. Nota-

[4]National Research Council, William Owens, Kenneth Dam & Herbert Lin, eds., Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities, § 9.1 (National Academes Press 2009).

[5]PDD/NSC-63, Critical Infrastructure Protection (May 22, 1998) [available at http://www.fas.org/irp/offdocs/pdd/pdd-63.pdf].

bly, the directive treated cyberspace as a *mode* by which threats to infrastructure would be propagated and did not identify cyberspace, itself, as a critical infrastructure asset. Each sector of the economy was to identify its vulnerabilities and propose remedies for them. The directive called for development of response plans to minimize the damage of attacks on infrastructure and reconstitution plans for restoring capabilities rapidly.[6]

PDD-63 also devised a coordination structure that has, in effect, become the model for all succeeding cyber defense and resilience activities. Within the Federal government, each economic sector was associated with a "lead agency" that would have the principal responsibility for coordinating activities with the private sector and developing the Federal plans. As one might expect, these designations followed the regulatory functions of then-existing Federal agencies: Treasury was the lead for banking activities; HHS for public health; Energy for electric power and so on.[7] These agencies would appoint senior officials to serve as "Sector Liaisons" who would, in turn be coordinated by a "National Coordinator for Security, Infrastructure Protection and Counter Terrorism" who would, himself, be a subordinate of the National Security Advisor (that is, part of what today we would call the National Security Council). The work of this Federal organization would be supplemented by the appointment of a board of prominent non-Federal leaders (infrastructure providers and state and local officials) who would provide advice under the auspices of the National Infrastructure Assurance Council (NIAC), a board that continues to exist today.[8]

ISACs

As a direct result of PDD-63, the U.S. government fostered the creation of sector-specific Information Sharing and Analysis Centers (ISACs). The purpose of the ISACs, as the name suggests, is to enable the sharing of information, within each sector, about threats and vulnerabilities to that sector. Since 1998, ISACs have been created in many of the critical infrastructure sectors (e.g. Financial Services; Real Estate; and Electricity). Most notably, an Information Technology ISAC was one of the first created. The current reach of the ISACs to the various critical infrastructures is extensive. When considered collectively, the individual private/public sector ISACs possess an outreach and connectivity network to approximately 85% of the U.S. critical infrastructure.

The ISAC structure is intended to provide each sector with 24/7 information sharing/intelligence capabilities; allow the sector to collect and analyze threats based on its own subject matter analytical expertise; and coordinate with the government on sector-specific impacts. The efforts have been moderately successful in disseminating information, but complaints from industry continue to arise that the government is not effectively using private sector expertise to leverage its capabilities,[9] and does not (often for classification reasons) adequately share threat information in the cyber domain.[10]

---

[6]PDD/NSC-63 §8.

[7]PDD/NSC-63, Annex A.

[8]PDD/NSC-63 § VI.

[9]For example, initially few, if any, private sector participants were routinely invited to the large-scale TOPOFF exercises in which U.S. government officials examine their response to predicted future terrorist incidents. *See* ISAC Council White Paper, "The Integration of ISACs in to Government and Department of Defense Homeland Security and Homeland Defense Exercises, (January 2004) [available at http://www.isaccouncil.org/whitepapers/files/Integration_of_ISACs_Into_Exercises_013104.pdf]. Though this particular issue has been resolved in more recent exercises it is emblematic of the challenges faced in integrating a public and private sector response.

[10]There have been no significant recent studies of the effectiveness of ISACs by outside sources. A dated review, conducted by GAO in 2005, reports a number of breakdowns in information sharing. *See* Critical Infrastructure Protection: Department of Homeland Security Faces Challenges in Fulfilling Cybersecurity Responsibilities, at 32 (GAO-05-434 May 2005). A slightly more recent study from 2006 found that successful integration varied widely across the ISAC sectors. *See* Critical Infrastructure Protection: Progress Coordinating Government and Private Sector Efforts Varies by Sectors' Characteristics (GAO-07-39 Oct. 2006).

Recent Developments

President Bush sought to advance the Clinton initiative, and gave voice to the first "National Strategy to Secure Cyberspace."[11] For the first time, the strategy recognized that cyberspace was a separate infrastructure in its own right, worthy of protection because of its inherent value (rather than, as before, because it provided a means by which attacks on other infrastructure could occur). The principal noteworthiness of the strategy, for purposes of this inquiry, lay in its call for the development of a public-private architecture for responding to national cyber incidents.[12]

This recognition of the uniqueness of cyberspace as an independent infrastructure was confirmed in Homeland Security Presidential Directive (HSPD)-7, which defined critical infrastructure as "both physical and cyber-based" assets so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on American interests.[13] HSPD-7 sought to define the coordinating role of the Department of Homeland Security (DHS) in protecting cyber assets, directing the DHS Secretary to "maintain an organization to serve as a focal point for the security of cyberspace. The organization will facilitate interactions and collaborations between and among Federal departments and agencies, State and local governments, the private sector, academia and international organizations. To the extent permitted by law, Federal departments and agencies with cyber expertise, including but not limited to the Departments of Justice, Commerce, the Treasury, Defense, Energy, and State, and the Central Intelligence Agency, will collaborate with and support the organization in accomplishing its mission."[14]

As the laundry list of involved agencies makes clear, the coordinative function on cybersecurity issues is a daunting task. The challenge is magnified when one considers the multivariate nature of the tasks that comprise a government-wide approach to cybersecurity. In January 2008, President Bush adopted a Comprehensive National Cybersecurity Initiative (CNCI), portions of which were declassified by President Obama in 2010. The CNCI identifies 12 broad cybersecurity initiatives, ranging from increased cyber education and cyber domain situational awareness to a call for the development of a comprehensive cyber deterrence strategy (of which this study is a small part). All but 3 of these initiatives are fairly characterized as requiring efforts of cyber defense and/or cyber resilience.[15]

The complexity of the coordination task was highlighted by the principal recommendation of President Obama's Cyber Space Policy Review, a comprehensive review of American cyber policy undertaken at the start of the President's Administration.[16] Recognizing the difficulty of coordinating so many initiatives in so many agencies, the Review called for the appointment of a White House-level policy coordinator (colloquially knows as a "Cyber Czar") who would "anchor" leadership on cyber issues within the White House.[17] Indeed, the need for leadership was so palpable that the Review's first chapter was entitled "Leading from the Top." Responding to this call, in December 2009, President Obama appointed Howard Schmidt as the first Special Assistant to the President and Cybersecurity Coordinator.

The Cybersecurity Coordinator's powers remain, however, consultative and coordinative rather than directive and mandatory. As the Review made clear, the coordinator does not (and was not intended to) have any operational authority or responsibility, nor the authority to make policy unilaterally. Rather

[11]The National Strategy to Secure Cyberspace (February 2003), [available at http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf].

[12]National Strategy to Secure Cyberspace at 20-24.

[13]Homeland Security Presidential Directive-7 (Dec. 17, 2003).

[14]HSPD-7 § 16.

[15]Comprehensive National Cybersecurity Initiative (declassified version) [available at http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative]. Three of the initiatives (calling for a cyber counter-intelligence policy; development of a deterrence strategy; and adoption of a supply change risk management strategy) have aspects of cyber defense or resilience to them, but more appropriately are characterized as policies of cyber assurance, cyber attack or non-cyber response. As with any taxonomy, the categorization of policies is indefinite at the margins and of utility only insofar as it aids analysis.

[16]Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure (May 2009).

[17]Cyber Space Policy Review at 7; *see also id*. at vi (recommendation #1, calls for appointment of NSC-level policy cyber coordinator).

the coordinator is intended to act through the normal interagency process to harmonize and coordinate policy across inter-agency boundaries.[18] Here too, as the CNCI's task-list makes clear, the predominant effort for the Coordinator has been in the realms of cyber defense and cyber resilience.

B. Cyber Systems Assurance

Other cyber threats arise, not from direct attack on the system, but from threats that originate from within the system itself. Some of those threats might arise from insider activity—as when an enemy agent successfully poses as an insider to gain access to the cyber system. Conceptually, however, this insider threat (whether to a U.S. government target or a private commercial target) poses no problems distinct from those posed by any other insider effort. Likewise, the systems we have developed and put in place to protect against more traditional insider threats of espionage—security clearances and background checks—are likely also appropriate to counter the cyber insider threat. Thus, there is little reason to suspect that any organizational or process issues exist that are unique to cyber insiders.

The same cannot be said of the inside threat posed to cyber systems by the workings of the hardware within the various routers, switches, operating systems and peripherals that comprise the real-world manifestations of cyberspace or the code in the software purchased from foreign sources.[19] History records several examples where a state actor has taken advantage of its position as a system supplier to surreptitiously introduce systems subject to its own control or influence.[20] It is thus a matter of significant concern that over the past decades the United States government has become increasingly reliant on commercial off the shelf technology (COTS) for much of its cyber supply needs. Indeed, counterterrorism experts have sometimes opined that American reliance on COTS computer technology, that is often manufactured and/or maintained overseas, poses a greater vulnerability to U.S. cyber systems than traditional cyber attacks.[21] Or, as the Defense Science Board opined in 2007: "The current systems designs, assurance methodologies, acquisition procedures, and knowledge of adversarial capabilities and intentions are inadequate to the magnitude of the threat."[22]

The situation has changed little in the past three years. For this reason, the CNCI identified "global supply chain risk management" as one of the initiatives critical to enhanced cybersecurity.[23] Yet, the U.S. has a very limited set of systems and processes in place to respond to this challenge. Indeed, as observers have noted, there is a disconnect between our counter-intelligence, which is often aware of risks to our cyber supply chain, and our procurement processes, which cannot have access to classified information regarding supply chain threats. Setting aside intelligence concerns, the prospect of creating a "black list" of unacceptable products for purchase is fraught with problematic issues regarding liability

[18]Cyber Space Policy Review at 8.

[19]The dependence of the Department of Defense on commercial, non-domestic software and hardware was identified as a significant vulnerability by the Defense Science Board. *See* Report on Mission Impact of Foreign Influence on DoD Software (Defense Science Board, Sept. 2007). The vulnerabilities identified are not, of course, limited to DoD, but pervade any IT system (whether governmental or private-sector operated) that uses foreign-sourced hardware or software.

[20]A recent RAND study, for example, noted two such instances—the British "gift" of Enigma machines to other countries and a Russian use of black market systems controllers to disrupt pipeline activity. *See* Martin Libicki, Cyberdeterrence and Cyberwar, at 21 & nn. 27, 28 (RAND 2009).

[21]Libicki, Cyberdeterrence and Cyberwar at 22; National Security Threats in Cyberspace at 24-25 (ABA/National Strategy Forum, 2009 [hereinafter "National Security Threats"].

[22]Defense Science Board, "Foreign Influence," at vi.

[23]CNCI, Initiative #11. It bears noting that supply chain security is not exclusively an issue of national security. Many of the same problems and challenges are posed by the possibility of fraud and the delivery of counterfeit products. The magnitude of the problem is daunting. A recent Department of Commerce report cited nearly 9,000 instances of counterfeit electronics encountered by original component manufacturers in 2008 alone. *See* Department of Commerce, Bureau of Industry and Security (OTE), "Defense Industrial Base Assessment: Counterfeit Electronics," (Jan. 2010) at 11. The Semiconductor Industry Association has reported the seizure of more than 1.7 million counterfeit chips since its Anticounterfeiting Task Force began in 2007. *See* Michael Aisenberg, "The Information Technology Supply Chain: Survey and Forecast of Emerging Obligations for Industrial Vendors," at 2 (ABA Info Sec. Quarterly, Spring 2010) [copy on file with author].

and fidelity.[24] And, even if we could devise a means of giving the procurement process access to sufficient information and if liability issues could be overcome, it might well be the case that no significant alternative sources of supply exist.

At present, there are only two notable structures in operation within the U.S. government that provide a means of addressing supply chain security issues—and neither is particularly adept or well suited to the task.

One is the Committee on Foreign Investment in the United States (CFIUS). CFIUS is an inter-agency committee authorized to review transactions that could result in control of a U.S. business by a foreign person (known as "covered transactions"), in order to determine the effect of such transactions on the national security of the United States.[25] If CFIUS determines that the proposed transaction poses a risk of some sort it may prohibit the transaction altogether or, far more frequently, it may enter into a mitigation agreement that puts in place mechanisms and requirements that it deems necessary to ameliorate the risk. Though CFIUS was initially created to focus on the sale of companies that would result in foreign control of defense-critical industries, in the post-9/11 world it has come, as well, to focus on sales that will effect critical infrastructure (such as the now-infamous sale of port facilities to Dubai Ports World). This focus has, on at least one publicly acknowledged occasion, involved the review of a purchase that implicated cybersecurity concerns.[26]

Likewise, an interagency working group known as "Team Telecom" reviews questions relating to the acquisition of an ownership interest in American telecommunications companies by foreign interests. The Federal Communications Commission has statutory authority to review transactions where a foreign entity seeks to purchase more than a 25 percent indirect ownership stake in U.S. common carriers licensed by the FCC. When such a transaction is proposed the FCC will, as a matter of policy, defer to the Executive branch and coordinate the application with the Executive branch for national security, law enforcement, foreign policy, or trade concerns. The applications are referred to Team Telecom, which is co-chaired by staff from the Department of Homeland Security and the Department of Justice, including the FBI, and which also includes representatives from the Departments of Commerce, Defense, State, and the Treasury, and the Office of the United States Trade Representative. Based on its review, Team Telecom may have no comment on an application or may request that the FCC condition grant of the application on compliance with assurances made by the applicant in either an exchange of letters or a formal security agreement. In this way, as well, the U.S. government will on occasion have a process in place for addressing cyber assurance concerns that result from the foreign purchase (note that both processes are limited to the acquisition of ownership interests) of an interest in a cyber-related industry.[27]

In recent years a number of ad hoc working groups have sprung up to consider the COTS challenge. Many of them operate in a classified environment. A recent survey by the Co-chair of the ABA Information Security Committee identified no fewer than five separate industry and Federal initiatives.[28] The

[24]National Security Threats at 24-25.

[25]CFIUS operates pursuant to section 721 of the Defense Production Act of 1950, as amended by the Foreign Investment and National Security Act of 2007 (section 721) and as implemented by Executive Order 11858, as amended, and regulations at 31 C.F.R. Part 800. The DNI is tasked with conducting an intelligence assessment of the risks posed by certain transactions and reporting to the committee on his findings. His representative sits, *ex officio*, on the committee and brings a counter-intelligence perspective to its deliberations where appropriate.

[26]*See* James Jackson, "The Committee on Foreign Investments in the United States (CFIUS)" at 9 (Congressional Research Service, Feb. 4, 2010) (reporting that the Israeli firm Check Point Software Technologies decided to call off its proposed $225 million acquisition of Sourcefire, a U.S. firm specializing in security appliances for protecting a corporation's internal computer networks, because of a CFIUS inquiry). The author is personally aware of several similar transactions, the details of which are protected by the confidentiality rules that apply to CFIUS activities.

[27]One other, rarely used, mechanism is section 232 of the Trade Expansion Act of 1962 (19 USC. § 1862). Section 232 authorizes the Department of Commerce, in consultation with DoD and other appropriate agencies, *see* 15 CFR Part 705, to block the importation of goods that would displace domestically produced materials essential to the defense industrial base. Given the infrequency of its application, section 232 is of little practical import.

[28]Aisenberg, "Information Technology Supply Chain," at 1 & n.3, 6-8. The author is indebted to Michael Aisenberg of MITRE, whose comments on the initial draft of this paper allowed the development of the analysis in this section.

most notable are two recent data-collection initiatives documenting the extent to which counterfeits infiltrate our supply chain: a recently completed study by the Department of Commerce, which documented the prevalence of counterfeit parts in the Navy's IT supply chain,[29] and ongoing pilots within the CNCI, Task 11, collecting detailed data on vendors, components, product integration and deployment of cyber products within DoD and DHS.[30]

C. Cyber Attack and Non-Cyber Response

The U.S. military has moved aggressively to establish doctrine and structures for the control of military operations in cyberspace. The Army, for example, has developed a concept of operations and a set of capabilities requirements for military action in cyberspace.[31] Likewise, the Navy has created a Fleet Cyber Command and reactivated the 10th Fleet for cyber warfare.[32] Similarly, the Air Force has designated its existing Space Command as the locus for its cyberspace mission and has begun inculcating its Airmen with the need to be "Cyber Wingmen."[33]

To coordinate these sometimes disparate efforts, on June 23, 2009, the Secretary of Defense issued a memorandum creating a new command, the U.S. Cyber Command (USCC), within the structure of our military forces. More particularly, the Secretary created Cyber Command as a sub-unified command subject to the authority of the commander of the U.S. Strategic Command.[34] As detailed in section 18.d(3) of the DOD Unified Command Plan, the USCC is tasked with securing American freedom of action in cyberspace and mitigating the risks to national security that come from dependence on cyberspace. It is, therefore, the home of both offensive and defensive military cyber missions of all sorts. A catalog of its missions includes:

- integrating cyberspace operations and synchronizing warfighting effects across the global environment;
- supporting civil authorities and international organizations in cyberspace activities;[35]
- directing global information grid operations and defense;
- executing full spectrum military cyberspace operations;
- de-conflicting offensive cyberspace operations;
- providing situational awareness of cyberspace operations, including indications and warnings; and
- providing military representation to U.S. and international agencies on cyberspace matters.

In short, USCC is anticipated to serve as a broad-based, comprehensive locus for U.S. military cyberspace operations, with significant impact on non-military civilian operations. And, consistent with

[29]The report is summarized in a useful briefing, available at www.combatcounterfeits.com/files/bis-counterfeit-briefing.ppt.

[30]Aisenberg, "Information Technology Supply Chain," at 10.

[31]TRADOC PAM 525-7-8, Cyberspace Operations Concept Capabilities Plan (Feb. 2010).

[32]Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet (Jan. 29, 2010) [available at http://www.navy.mil/search/display.asp?story_id=50954].

[33]*See* Memorandum for All Airmen, Air Force Cyberspace Mission Alignment (Aug. 20, 2009).

[34]The new commander of USCC is dual-hatted and also serves as the Director of the NSA. A useful summary of the political considerations that led to this unusual result can be found in Richard A. Clarke & Robert K. Knake, Cyber War (Harper Collins 2010), pp. 32-44.

[35]Presumably this support to civil authorities will be provided consistent with existing military doctrine. DoD Directive 5111.13 (March 2009) defines Defense Support to Civil Authorities (DSCA) as: "Support provided by U.S. Federal military forces, National Guard forces performing duty in accordance with [Title 32, U.S. Code], DoD civilians, DoD contract personnel, and DoD component assets, in response to requests for assistance from civil authorities for special events, domestic emergencies, designated law enforcement support, and other domestic activities. Support provided by National Guard forces performing duty in accordance with [Title 32, U.S. Code] is considered DSCA, but is conducted as a State-directed action. Also known as civil support."

existing joint doctrine, the commander of USCC will, generally, have the freedom to select and approve specific courses of action to achieve the mission objectives set by his superiors.[36]

It is, of course, difficult to develop a concrete sense of what USCC actually will do. The command has not yet been fully activated and will not become so until October 2010. It was only recently, in May 2010, that its first nominated commander was confirmed by the Senate. Nor has the command developed a set of policies and doctrines that will guide its actions; its first comprehensive strategy is anticipated late in 2010.

Thus USCC is, ironically, a virtual command at this juncture and the most that can be said is that it appears to be quite flexible in its scope. The authorizing documentation provides DOD with ample ability to develop within USCC any number of cyber-related missions. With respect to cybersecurity matters (what this paper classifies as cyber defense and cyber attack) it is likely in the end that the limitations on the scope of activity in USCC will be more in the nature of resources and external competition with other U.S. government agencies, rather than inherent limitations in its authorities. In short, we have a new cyber command, but the policy and doctrine that will define its objectives remain to be better defined.

The military is not, of course, the only U.S. governmental institution that would be responsible for a cyber response. The dynamics of the domain will necessarily involve other governmental agencies in any cyberaction. To cite the most obvious example, as the Cyber Space Policy Review, the National Cybersecurity Strategy and the recent CSIS study on Securing Cyberspace all recognize, the internet is a uniquely borderless domain.[37] Thus any effective deterrent strategy will necessarily require a governmental organization and process that enables international engagement. While one could, in theory, imagine a situation in which all of our cyber responses were enabled by military-to-military interactions the prospects for such a scenario are dim. Rather, one can readily anticipate that international engagement will require engagement across the domain of diplomacy, law enforcement and infrastructure protection, with a necessarily wide variety of international interlocutors.

Likewise, our government's cyber capabilities are not only useful as a cyber response measure. They may well play a role when kinetic military strikes would be viewed as too drastic or disproportionate, or even as a response to diplomatic disagreements, both overtly and covertly. And, of course, these capabilities can and will be used as a tool to supplement more traditional military operations to disable an enemy's command and control structures. We have only begun our efforts to build the structures necessary to direct these multiple missions.[38]

---

[36] *See generally*, Unified Command Plan § 18.d(3); Advanced Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command in Hearings Before the United States Senate Armed Services Committee (April 13, 2010) [available at http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf] [hereinafter "Alexander, Advanced Questions"].

[37] National Security Strategy at 49-53; Cyber Space Policy Review at 20-21; CSIS, Securing Cyberspace for the 44th Presidency at 20-23 (Dec. 2008).

[38] No description of the organizations and processes necessary for cyber deterrence would be complete without acknowledgment of the need for structures to ensure that activities intended to prevent a successful cyber attack by U.S. opponents or to enable a successful cyber attack by our own government are pursued in conformance with the laws and policies of the United States. As other papers in this collection make clear, a number of potential activities in support of a cyber deterrence policy have significant privacy and civil liberties implications.

This paper consciously leaves aside this very significant implementation question, though it is clearly one that *must* be addressed. Existing oversight structures range from agency level privacy officers and inspectors general to executive level institutions such as the Intelligence Oversight Board of the President's Intelligence Advisory Board (established by E.O. 13462), and the Privacy and Civil Liberties Oversight Board (created by Pub. L. 110-52, 9/11 Commission Act, § 801, though as of the writing of this paper inactive). These executive mechanisms are supplemented through congressional oversight and, where appropriate, judicial review of executive actions. As new deterrence policies are developed and implemented it is likely that new privacy protective systems will also be developed (indeed, this paper suggests one such system as part of its description of a new public/private model of cooperation). This paper does not, however, provide a complete description of existing structures. The failure to address the question, however, is by no means a diminishment of its importance.

II. CHALLENGING QUESTIONS—THINKING ABOUT ORGANIZATION AND PROCESS

Most are familiar with the unique aspects of cyberspace that make a deterrence policy challenging to develop. The difficulties of attributing an attack to a particular actor are well-documented. Likewise, the independence (or purported quasi-independence) of certain cyber actors from state sponsors further complicates the equation of attribution, and the surreptitious nature of some intrusions often makes attacks difficult to perceive (and thus respond to).

But the particular challenges for conceptions about the organization and processes of the U.S. cyber deterrence policy lie not in these difficulties, for they are more technological than organizational. They will likely not be resolved by a decision on how the government and private sector are organized. Put another way it is hard to imagine how an organizational change in the U.S. government would increase (or decrease) our ability to resolve the attribution question on a routine basis.

Rather, for purposes of this paper, it is useful to consider difficulties that particularly give rise to organizational challenges in our defense of cyberspace. Given the uncertainties surrounding the cyber realm and its rapidly mutating nature, no paper of any reasonable length can identify, much less address, all of the salient organizational challenges. Below, this paper offers thoughts on six issues—the failure of the market; the assumption of the need for a rapid response; the asymmetry of risk; the challenge of hardware reliance; the disablement of private self-help; and unseemly federal competition.

A. The Public/Private Dilemma

The fundamental question is: Who should be responsible for protecting the cyber domain? Why, after all, are cyber defense and resilience even a matter of governmental concern? Ought we not to anticipate that the private sector would address these matters on its own initiative? With over $1 trillion in losses from cyber theft annually,[39] a traditional theory of the efficient market would posit the development of a robust market for security solutions.

This has not been the case. Rather, the prevalence of security vulnerabilities in the system appears to reflect a systematic market failure.[40] Because the costs of inadequate security are often (though not always) borne by the customers of the cyber service provider (rather than the provider itself), the costs of security failures are, quite naturally not internalized by private sector actors in a way that incentivizes them to take adequate protective steps. Security for the broad system of the internet (both its private components and the government components) is a classic market externality whose pricing is not adequately captured in the costs experienced by individual users. The situation will only get worse: "there is widespread agreement that this long-term trend of grabbing the economic gains from information technology advances and ignoring their security costs has reached a crisis point."[41]

The difficulty in developing a private cybersecurity solution is exacerbated by systematic limitations on information sharing necessary to combat cyber threats. Private enterprises have little incentive to publicly identify their own vulnerabilities. This is especially true in the cyber domain, where the private sector actors are notoriously distrustful of government interference and regulation. And the converse is also true—government institutions like the NSA with (perhaps) superior knowledge of threat signatures and new developments in the arsenal of cyber attackers are deeply reluctant to share their hard won knowledge with the private sector at the risk of compromising their own sources and methods. At this

[39]Elinor Mills, Study: Cybercrime Costs Firms $1 Trillion Globally, CNet.com (Jan. 28, 2009) [available at http://news.cnet.com/8301-1009_3-10152246-83.html].

[40]National Security Threats at 11-14. An extended discussion of cyber space as a "commons" can be found in Rattray, Evans & Healey, "American Security in the Cyber Commons," *in* Denmark & Mulvenon, eds., "Contested Commons: The Future of American Power in a Multipolar World" (CNAS Jan. 2010).

[41]Jack Goldsmith and Melissa Hathaway, "The Cybersecurity Changes We Need," Washington Post (May 29, 2010) [available at http://www.washingtonpost.com/wp-dyn/content/article/2010/05/28/AR2010052803698.html].

point, the sad truth is that, despite efforts within the ISACs, we have yet to successfully develop the political will to create the culture where information sharing enables cybersecurity improvement.

This has led some to contemplate organizational changes that would enable the Federal government to take direct responsibility for securing the cyber domain. At present, Federal organizations exist for this purpose but the scope of their activities is limited: the Department of Homeland Security has begun deployment of an intrusion detection system (known as Einstein 2) to protect the .gov domain and has started the development of an intrusion prevention system, called Einstein 3.[42] The military has taken similar steps to protect nodes on the .mil domain. One can at least conceptually envision a Federal organization that would deploy the same sorts of protective technology on private sector portions of the internet to protect the civilian domains (.com, .net., and .edu). Indeed, given that government traffic is often dependent on the private sector network for transmission, some (including, most recently, the Deputy Secretary of Defense) have expressed the view that Federal protection of private sector networks is affirmatively desirable for governmental purposes, independent of any benefit to the private sector.[43] Such an organization, if created, would eliminate some of the information sharing problems but would bring with it a host of privacy-related concerns that might prove insurmountable, for it would place the Federal government in the position of monitoring and controlling private sector internet traffic.

Indeed, to summarize the problem, a *government operated* system will raise the specter of "Big Brother" and engender significant opposition from privacy advocates, while a *privately operated* system has proven impossible to develop naturally, lacks transparency, and has less ready access to NSA-generated threat signature information. If we do not solve the dilemma of enabling public-private cooperation we are unlikely to get cyber defense and cyber resilience right.[44]

B. The Assumption of Rapidity

One of the unique aspects of cyberspace that will particularly affect our organizational structures and processes is the *rapidity* with which cyber activities occur. When a cyber domain attack is perceived to occur at the pace of milliseconds, it may be that the deterrent or defensive response will need to occur with equal rapidity. As LTG Keith Alexander, the first Commander of U.S. Cyber Command, recently told the Senate, "[A] commander's right to general self-defense is clearly established in both U.S. and international law. Although this right has not been specifically established by legal precedent to apply to attacks in cyberspace, it is reasonable to assume that returning fire in cyberspace, as long as it complied with the law of war principles (e.g. proportionality), would be lawful."[45] We therefore face a situation where it is possible (indeed, likely) that some subordinate commanding officer may feel compelled (and authorized) to act without higher authorization if the commander perceives that a cyber attack has

[42]Privacy Impact Assessment for the Initiative Three Exercise, DHS Privacy Office (March 18, 2010) [available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3.pdf].

[43]*See e.g.* William J. Lynn, III, "Defending a New Domain: The Pentagon's Cyberstrategy," 97 at 104 (Foreign Affairs, Sept./Oct. 2010) (recommending that policy makers consider extending NSA intrusion detection and prevention capabilities "beyond the .gov domain" to, for example, domains "undergirding the commercial defense industry").

[44]One final complexity deserves mention at this juncture—nobody actually owns or operates the Internet itself. While private sector and government actors own pieces of the cyber domain (various routers and nodes, for example) the actual rules for how the cyber domain works are set by the Internet Engineering Task Force which is an "open international community of network designers, operators, vendors and researchers concerned with the evolution of the Internet architectures and the smooth operation of the Internet." "Overview of the IETF" [available at http://www.ietf.org/old/2009/overview.html]. This community operates by the promulgation of technical standards which, in the end, become *de facto* operating requirements for any activity in cyberspace. Thus, some questions about cyber defense and resilience may, necessarily, require engagement with an engineering community that is both internationalist and consensus-oriented, characteristics that may be inconsistent with effective U.S. government action.

[45]Alexander, Advanced Questions at 24; *see also* Lynn, "Defending a New Domain," at 103 (U.S. military must "respond to attacks as they happen or even before they arrive").

begun. And what is true for the military may also be true of private actors who are protecting their own networks—they may feel the need to act instantaneously without the benefit of reflection.

This perception of the need for rapidity reflects a sea-change in concept. The physics of the internet destroys time and space.[46] Even in the nuclear domain, the imminence of the threat was measured in minutes, allowing the development of processes (like the classic nuclear code "football") that permitted a considered, albeit hurried, human response. The cyber domain is often characterized as one in which a near-instantaneous response is necessary.

That characterization may not, however, be accurate and its prevalence may actually be pernicious. A counter-response may be essential immediately as a purely defensive measure, but it is likely that a deterrence-based cyber response can be delayed without significant cost. As Martin Libicki pointed out in a recent RAND study, a cyber response is unlikely to be able to disable a cyber attacker completely. As a consequence, for deterrence policy, "[m]ore important than [the] speed [of the response] is the ability to convince the attacker not to try again. Ironically, for a medium that supposedly conducts its business at warp speed, *the urgency of retaliation is governed by the capacity of the human mind to be convinced, not the need to disable the attacking computer before it strikes again.*"[47]

This is a central insight that ought to govern organizational structures for U.S. cyber deterrence policy. Our task is relatively simple to describe (though difficult, in practice, to achieve);

- Begin, by dividing potential decisions into:
  - those that may require immediate action (e.g. rapid military cyber defense or attack); and
  - those for which time may be taken (non-military responses, for example, or long-term cyber resilience initiatives)
- For those decisions requiring either long-term preparatory action, or less rapid response, put in place purpose-built organizations and institutions to achieve defined objectives and provide adequate leadership and resources to achieve those ends;
- For those decisions that will require immediate action, set up structures now to permit consideration of "pre-approved" responses to anticipated situations; and
- In the absence of pre-approved responses, determine in advance who will make the necessary immediate decisions.

In short, in the case of cyber deterrence policy, perhaps function should follow form. The purpose of our organization should be to slow the responsive system down, where feasible, to allow consideration of alternatives and, where not feasible, to allow the prior consideration of response scenarios in advance of the need to implement the response. The worst of all possible worlds would be a lack of structure that permitted mature and thoughtful consideration of reasonable alternatives.

C. Risk Asymmetry

It is a relatively uncontroversial assessment of the current state of affairs to say that, in the cyber domain, the risk to the U.S. is asymmetric. Our nation, with its highly technology-dependent systems,[48] is comparatively more vulnerable to cyber attack than are many of our nation-state peer adversaries. And our comparative vulnerability is significantly greater than that of many non-state actors.

---

[46]Remarks of Kim Taipale, Duke University Center on Law, Ethics and National Security (April 2010) [available at http://www.law.duke.edu/lens/conferences/2010/program].

[47]Libicki, Cyberdeterrence and Cyberwar at 62 (emphasis supplied).

[48]The military, alone, has over 15,000 networks and 7 million computing devices. Its systems are probed thousands of times and scanned millions of times each day. *See* Lynn, "Defending a New Domain" at 97-98. Multiply that by the vulnerabilities in other Federal departments (not to mention State, local, and private sector networks) and the scope of the problem becomes impossibly daunting.

We have yet, however, to internalize the implications of this asymmetry for deterrence organization and policy. Our conception of deterrence is effected by memories of the Cold War, where the threat and response were relatively symmetric. We assumed that a nuclear attack would merit a nuclear response.

But there is no reason to believe that a cyber attack of any form *necessarily* requires a directly proportionate cyber response. Indeed, given the reality of asymmetric cyber reliance by our adversaries, the implication is that our response to a cyber attack should not be confined to a cyber response. While it is likely (indeed, almost certain) that a cyber-based response will form a portion of any deterrent strategy, it is equally likely (indeed, also equally certain) that our actions will engage the full panoply of U.S. governmental authority—ranging from economic sanctions to diplomatic endeavors, to espionage, to criminal prosecution and even to non-cyber kinetic military responses as the circumstances may require.

In a recent speech on internet freedom, Secretary of State Clinton emphasized this point, suggesting the broad scope of potential United States responses to cyber threats: "States, terrorists, and those who would act as their proxies must know that the United States will protect our networks. Those who disrupt the free flow of information in our society or any other pose a threat to our economy, our government, and our civil society. Countries or individuals that engage in cyber attacks should face consequences and international condemnation. In an internet-connected world, an attack on one nation's networks can be an attack on all. And by reinforcing that message, we can create norms of behavior among states and encourage respect for the global networked commons."[49]

And yet, at this juncture, the structures for a coordinated whole-of-government response to cyber threats and for the delivery of a non-cyber response are immature. A recent GAO study made clear that the White House has retained fairly tight control of the development of any deterrence strategy, assigning responsibility for the task directly to the National Security Council (rather than, say, assigning it to a DoD/State working group for development).[50] But, as the vignette which opened this paper makes evident, the White House-coordinated structures have yet to develop a doctrine for the expression of cyber policies.

What is necessary is a structure and organization that will allow the entire panoply of governmental responses to be considered (below, the author suggests a response to the need for such a structure—creation of a "Cyber Defense Options Group"). These will range across the entire domain of Federal activity (often requiring international cooperation) and could include (and this is just a sampling of possibilities):[51]

- *Public exposure and shaming*—The United States might, for example, publicize data and information identifying cyber intrusions and countries whose weak or ineffective civil justice system permits or fosters illegal activity;
- *Diplomatic condemnation*—We could work to develop international norms of behavior, including cooperation in the suppression of cyber intrusions, and then use diplomatic processes to develop shaming techniques that might modify state-actor behavior;
- *Economic sanctions*—One can readily imagine a role for economic sanctions in response to cyber intrusions. For example, one might impose retributive tariffs on non-cooperative countries. More aggressively one might boycott or blacklist products from countries known to introduce malicious hardware into COTS technology, and seek to convince other nations to adopt similar sanctions;

[49]Speech of Secretary of State Hillary Clinton (Washington DC Jan 21, 2010) [available at http://www.state.gov/secretary/rm/2010/01/135519.htm].

[50]GAO, "Cybersecurity: Progress Made But Challenges Remain in Defining and Coordinating the Comprehensive National Initiative," at 13 (GAO-10-338) (March 2010) [hereinafter "GAO Cybersecurity"].

[51]Current conceptual thinking in conflict management broadly recognizes that "soft power" systems will often be effective supplements to the hard power of a kinetic response. *E.g.* Joseph Nye, Soft Power: The Means to Success in World Politics (Public Affairs 2004). Theorists characterize the panoply of soft power instruments through the mnemonic "MIDLIFE"—that is Military; Intelligence; Diplomacy; Law enforcement; Information; Financial; and Economic instruments of power. All, conceivably, could be of use in deterring cyber attacks and intrusions.

- *Cyber sanctions*—Sometimes cyber acts will beget cyber sanctions. If a country persists in misusing internet domain name directories, for example, international organizations might, in turn, limit or restrict the development of new domains within that country. More extreme sanctions (for example, bandwidth throttling) are also conceivable;
- *Financial punishments and criminal sanctions*—Administrative, civil and criminal sanctions may be available in situations where an actor (or an intermediary) may be readily identified. In traditional conceptions of deterrence theories, these sorts of sanctions are considered effective as a response to malfeasant individual conduct;
- *Expulsion from international organizations*—In conjunction with any of these sanctions one might, in significant cases, consider suspending or expelling a country from relevant international organizations as a sanction for its activities (or those within its borders);
- *Espionage and other covert responses*—Naturally, one response to covert cyber activities will be covert activities by America. Indeed, it may well be that covert cyber activities will be a critical enabler for the effective implementation of other whole-of-government responses, providing essential intelligence to enhance effective targeting of the response;
- *Cyber intrusions or attacks*—Of course the fact that other responses are possible does not mean that a cyber response is inappropriate. It may often be the case that a like-for-like cyber response will be deemed to have the maximum deterrent effect while achieving proportionality;
- *Kinetic military attacks*—And, finally, there is no reason to suppose that a cyber attack with kinetic or near-kinetic effects on American targets must, necessarily, be responded to with an equivalent cyber response. It is at least plausible to consider the possibility that a traditional kinetic response will be the more proportionate and responsible one.

Our organizational structures and processes must be designed to accommodate and foster the consideration of these various options. Contrast that with our nuclear deterrence structures which were principally intended to verify that an attack had been launched and allow the President the opportunity to respond if he deemed it necessary. Indeed, one of the lessons from our experience with nuclear deterrence is that often the lens through which response actions can be taken needs to be broadened (as it was, for example, in our response to the Cuban missile crisis). In the cyber domain, the need to institutionalize that broadening of response will likely be even greater. Our structures must provide for a less focused response and allow for the consideration of all feasible action options. Instead of narrowing the structure and focusing on a single decision the cyber response structure must be necessarily more diffuse, lest we run the risk of conceiving of the cyber domain in predominantly military terms and thus militarizing a fundamentally civilian environment.

There are, of course, likely to be costs to this broadening. Most notably, it risks frustrating decision-making altogether. But if the structures and processes are properly defined and well-led, that challenge can be overcome. And the virtues of a whole-of-government response likely outweigh the costs associated with a more complex decision-making process.

D. Hardware Failures

If you ask counter-intelligence experts which they fear more, American vulnerability to an external cyber attack or the potential compromise of the operation of the hardware innards of our computers and internet switches, they almost certainly will say that the hardware threat is more challenging. The globalization of production for both hardware and software makes it virtually impossible to provide either supply chain or product assurance.[52]

The vulnerability is made acute by the fact that the U.S. government (and the private sector) have come to rely on commercial off-the-shelf technology. These COTS technologies have many obvious

[52]National Security Threats at 2. The observation as to the prioritization of threats was made by a participant whose comments were subject to Chatham House rules—they were for the public record but not for direct attribution.

advantages—they are generally cheaper than custom-built proprietary solutions and, because they are produced in the private sector, they are modified and upgraded more rapidly in a manner that is far more consistent with the current technology life-cycle. Particularly in the cyber realm, where upgrades occur with increasing frequency, reliance on COTS allows government and the private sector to field the most modern equipment possible.

One example of the COTS phenomenon, as recounted by an International Telecommunications Union workshop, will serve as an example: "In the mid-1980's, the DoD mandated the use of the ADA programming language. ADA never gained popularity in the commercial sector, which evolved from programs such as Cobal and Fortran to C and C++ as common programming languages. While ADA was optimized for real time and rapid conversion of analog to digital information, much faster microprocessors and digital sensors circumvented most of these advantages."[53] As a consequence ADA fell into disuse and the DoD systems moved away from their specially designed, non-commercial programming language to a commonly available commercial one. But, in doing so, the U.S. adopted a structure where it was vulnerable to the same types of attacks and hacking as commercial systems. The vulnerabilities that come from running commercial operating systems on most government computers would not exist in the same way if our computers operated on a non-commercial system.[54]

This is equally true for our hardware purchases. Because COTS systems have an "open architecture" design few of them have integrated security architecture. Increasingly, knowledge of the design of the systems and their manufacture is outsourced to overseas production. We therefore live in a world where a significant fraction of the innards of our computers are manufactured overseas, often in plants located in peer-competitor nation states.[55] Likewise, much of the service of existing systems is conducted overseas.

A process for dealing with these vulnerabilities is by no means clear. It is unlikely that the United States government and private sector will return to a time when all of its systems were "made in the USA." Doing so would be prohibitively expensive and would forego a substantial fraction of the economic benefits to be derived from the globalization of the world's economy.

A "made in the USA" response would not eliminate the COTS problem, as even hardware constructed in the United States could be built with malicious intent. However, the origin of hardware components may create a significant difference in the nature of the problem. For U.S.-built components the threat is in the nature of an insider threat and we can have reasonable confidence that the quality control and security processes of the U.S.-domiciled manufacturer are intended to negate that threat, rather than foster it. For non-U.S. companies the same will often be true, at least for components manufactured in countries that take an equivalent approach to hardware assurance. But we may sometimes have less confidence in the efficacy of those processes in countries where quality control and security are less well-developed. Even more troubling, we may sometimes reasonably doubt whether the company's processes are truly designed to achieve those goals or whether the intent works at cross-purposes with America's interests. It is significantly more difficult for the inspection processes of the purchaser to provide for hardware or software assurance than it is for those of the manufacturer.[56]

---

[53]A Collective Security Approach to Protecting the Global Critical Infrastructure at 13 n.14 (ITU Workshop on Creating Trust in Critical Network Infrastructures, Document CNI/09, May 2002).

[54]It is true that all operating systems necessarily have vulnerabilities, and that would be true of government systems that run on ADA, or Windows, or Linux. The degree of comparative vulnerability of these operating systems is hotly debated. *See, e.g.,* Geer et al., Cyber*In*security: The Costs of Monopoly (available at http://cryptome.org/cyberinsecurity.htm) (arguing that monoculture of Microsoft Windows increases vulnerability). The point here is a much more limited one—when the operating system is constructed exclusively by the government, then the government has much greater control against the deliberate insertion of vulnerabilities and it will tend to minimize the extent to which it is subject to non-purposeful malware attacks.

[55]DoD has reported finding counterfeit hardware in systems that the Pentagon has purchased. *See* Ellen Nakashima, "Defense Official Discloses Cyberattack," Wash. Post (Aug. 24. 2010) (available at http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406154.html?hpid=topnews). The Army's concept of cyber operations for the future recognizes the need to address hardware vulnerabilities. *See* TRADOC PAM 515-7-8 at 12.

[56]Lynn, "Defending a New Domain" at 101 (hardware tampering is "almost impossible to detect and ever harder to eradicate").

And so, though the continued purchase of COTS from a globalized supply chain is inevitable, it would be inappropriate to disregard the threat posed by the foreign origin of much of our hardware. And, notably, the risk is not posed simply by the hardware purchases we make. Many of the service functions that our cyber domain requires are also procured from foreign providers. The commonplace chestnut is the complaint that all of the help lines are answered in India, but the far more significant fact is that many of the repair and maintenance services used for our cyber systems are also provided by foreign suppliers—and so the risk is not just that we purchase hardware from overseas sources but that we rely on those same sources for much of our operational repair and maintenance capacity.

The Comprehensive National Cybersecurity Initiative recognized this vulnerability with its initiative to "develop a multi-pronged approach for global supply chain risk management." But "multi-pronged approach" is often code for "this is a very big problem that we don't have a handle on." Thus, it is somewhat distressing (though utterly unsurprising) that the CNCI initiative to address this problem consists of little more than anodyne platitudes: "This initiative will enhance Federal Government skills, policies, and processes to provide departments and agencies with a robust toolset to better manage and mitigate supply chain risk at levels commensurate with the criticality of, and risks to, their systems and networks."[57] Far more concrete action is necessary, perhaps even action that is moderately intrusive on the free flow of globalized commerce.

E. The "Right" of Self-Defense

The failure to develop structures that effectively protect the private sector from cyber intrusion creates a challenge for private sector actors who are obliged to defend their own networks: Consider the cyber deterrence problem from the perspective of the private sector actor whose systems are subject to an attack. The vulnerability is particularly acute as we come to realize that our adversaries *may* be planning acts that are designed to target private infrastructure.[58] Private sector actors who are contemplating a response to such attacks may well find themselves on the horns of a dilemma—neither able to rely on the government to defend them nor legally authorized to respond themselves.

As with other actors in the cyber domain those defending private sector networks will frequently be unaware of the identity of their attackers, and they may often be equally unable to distinguish a true attack from a probe or an unlawful intrusion. In such an ill-defined situation, those who act in response to an attack may do so in violation of law. The Neutrality Act makes it illegal for an American to wage war against any country at peace with the United States.[59] It preserves, at least in theory, the power of the Congress to declare war and the monopoly power of the Executive to use force in the face of an external attack. Similarly, the Logan Act,[60] forbids American citizens from negotiating with foreign governments. It, too, is intended to preserve an zone of exclusive Federal policy control. Both Acts provide, in theory, for punishment as felonies.

---

[57]CNCI Initiative #11.

[58]Most notably, in recent months Congress has heard testimony about Chinese research that examines the possibility of creating a cascading failure in American electrical grids. *See* Wang & Rong, Cascade-based Attack Vulnerability on the U.S. Power Grid, 47 Safety Science 1332 (2009) [available at http://www.docstoc.com/docs/30535594/Cascade-Based-Attack-Vulnerability-on-the-US-Power-Grid%E2%80%9D].

[59]In its present form, the Act provides: "Whoever, within the United States, knowingly begins or sets on foot or provides or prepares a means for or furnishes the money for, or takes part in, any military or naval expedition or enterprise to be carried on from thence against the territory or dominion of any foreign prince or state, or of any colony, district, or people with whom the United States is at peace, shall be fined under this title or imprisoned not more than three years, or both." 18 USC. § 960.

[60]"Any citizen of the United States, wherever he may be, who, without authority of the United States, directly or indirectly commences or carries on any correspondence or intercourse with any foreign government or any officer or agent thereof, with intent to influence the measures or conduct of any foreign government or of any officer or agent thereof, in relation to any disputes or controversies with the United States, or to defeat the measures of the United States, shall be fined under this title or imprisoned not more than three years, or both." 18 USC. § 953.

But a private sector actor may well, either purposefully or perhaps even through inadvertence or mistake, trench upon these prohibitions.[61] Leaving aside whether a particular cyber response is a "military expedition" (i.e. a use of military force—which is, in fairness, a significant question), it is entirely plausible that a private sector response to an intrusion may involve taking action against a state actor or a quasi-affiliated state-sponsored entity. More commonly, it might involve communicating with the state actor in a way that could be construed as a "negotiation." Thus, a private sector actor might well be responsible for firing the first shot of a cyber war or conducting the first cyber negotiation. Put more prosaically, how should a private electric company react if its grid appears to be subject to infiltration from an unidentified Chinese source? Is it disabled from taking action by the potential that the foreign source might be operating at the direction of Chinese authorities?

Likewise, under the Computer Fraud and Abuse Act (CFAA), it is a crime to intentionally access any protected computer (that is one used in or effecting interstate or foreign commerce) without authorization, or in excess of authorized access, and thereby obtain information from the computer.[62] Since almost invariably, any protective action by a private sector actor will involve accessing a protected computer without authorization and obtaining information from it, virtually every aspect of private sector self-help is, at least theoretically, a violation of the CFAA and therefore a crime. The specter of criminal prosecution may disable or deter private sector self-help and may also have the effect of causing the private sector to outsource protective activities overseas.[63]

But the other side of the equation is equally troubling. Private sector actors will engage in self-defense when they have to, at least in part because they cannot (and currently do not) rely on the U.S. government as a protector. In the context of kinetic warfare it is quite reasonable to insist upon a governmental monopoly on the use of force. The Constitution, after all, charges the government with the obligation to "provide for the common defense" and, by and large, the Federal government has taken on that role in the kinetic sphere. Thus far, however, it has not done so in the cyber domain, and its failure to do so leaves private sector actors with no good option. If the government cannot provide for a defense (whether because it chooses not to or because it lacks the organization and structures to do so), it seems deeply problematic to prevent private sector actors from using whatever tools they have available to protect themselves.

F. Federal "Competition"

Given the many challenges faced by the Federal government, it is unsurprising that some see a continuing lack of adequate coordination at the Federal level in our cyber resilience and, particularly, defense activities. As the GAO reported earlier this year, though several coordinating groups exist at the White House, agencies continue to have "overlapping and uncoordinated responsibilities for cybersecurity activities."[64] To the extent the lack of coordination is discussed publicly, the perception is that there is an ongoing fight for control of the domestic cybersecurity effort pitting the National Security Agency against the Department of Homeland Security.

The perception of, at best, a lack of coordination and, at worst, continuing conflict over control of the cyber defense mission is only exacerbated by acts which at least facially suggest a continuing dissonance. A recent example was the announcement by NSA in October 2009 that it was breaking ground on a new facility in Utah to provide "intelligence and warnings related to cybersecurity threats,

[61]The analysis in this section was spurred by a question posed at a recent conference by Stephen Dycus, a member of the National Research Council committee that oversaw this project.

[62]18 USC. §1030(a)(2)(C).

[63]It is notable, for example, that the private sector efforts to track the Chinese intrusion into the Dali Lama's computer system (known as GhostNet) were conducted by a Canadian company. *See* Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor (Mar. 29, 2009) (available at http://www.scribd.com/doc/13731776/Tracking-GhostNet-Investigating-a-Cyber-Espionage-Network).

[64]GAO, Cybersecurity at 2.

cybersecurity support to defense and civilian agency networks, and technical assistance" to DHS. In November 2009, DHS opened its own new facility, the National Cybersecurity and Communications Integration Center, in Arlington, Virginia. This facility will "house the National Cyber Security Center, which coordinates cybersecurity operations across government, the National Coordinating Center for Telecommunications, which operates the government's telecommunications network, and the United States Computer Emergency Readiness Team, which works with industry and government to protect networks and alert them of malicious activity."[65] The two new facilities are, at least facially, somewhat duplicative (both, for example, purport to have a warning and alert function and both also anticipate assisting civilian networks in protecting themselves against attack) and indicative of a continuing need for strategic level cyber coordination.

Duplicative effort and the waste it entails are not the only risks posed by uncoordinated Federal activity. There may well be instances where the division of responsibility impedes essential information sharing of threat signatures (as the discussion of the ISACs above suggests). There may also be occasions where the comparative lack of transparency at NSA precludes effective oversight and control of executive activity by the legislative branch and the public.[66] But perhaps most significantly, the lack of coordination reflects an inability to bridge a cultural gap between the operational environment of the private sector and that of the national security environment. To be sure, DHS as an institution does not fully reflect the robust, competitive private sector environment of Silicon Valley. But allowing NSA or CyberCommand to have the predominant role will, inevitably bring a more militarized or intelligence-focused perspective to the problem than would be the case if the civilian DHS agency had a primary role. Thus, it matters significantly which agency is assigned as the lead for protecting civilian networks. As Rod Beckstrom (former Director of the DHS National Cybersecurity Center) noted, which agency leads the cybersecurity effort makes a difference because an "intelligence culture is very different from network operations or security culture."[67]

To some degree the dissonance between DHS and NSA activities is a product of a significant disparity in their resources and expertise. As the DHS Inspector General recently reported, DHS/US-CERT lacks both the authority to compel other federal agencies to follow its recommendations and the staff to adequately conduct operations.[68] The NSA, by contrast, is well-funded and staffed and has, within the domain of its own operations, ample authority to act—authority that has only been enhanced by the creation of CyberCommand. Indeed, despite DHS's statutory authority and responsibility for protecting civilian infrastructure it appears that it is NSA (and not DHS) that has begun a program, called "Perfect Citizen," to detects cyber assaults on private infrastructure.[69] Though details of this new program are hazy[70] it appears possible that the program will conflict with or duplicate programs operated by DHS. It may also presage an effort by NSA and the Pentagon to exert more control over civilian networks generally.

At present, the White House cyber coordinator lacks the authority to de-conflict these competing structures. His role, avowedly, lacks any authority over operational decisions or budgetary priorities.

---

[65]J. Nicholas Hoover, "NSA to Build $1.5 Billion Cybersecurity Data Center," Information Week (Oct. 29, 2009) [available at http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=221100260].

[66]This brief paper is neither the time, nor the place, to debate recent controversies over NSA activities. Suffice it to say that the controversies are real, and the public confidence in NSA's rectitude comparatively diminished.

[67]*See* Letter from Rod Beckstrom to Janet Napolitano (March 5, 2009) [available at http://epic.org/linkedfiles/ncsc_directors_resignation1.pdf]. Beckstrom resigned his position as Director of the National Cybersecurity Center in part because of his perception that NSA was, inappropriately "control[ing] DHS cybersecurity efforts." *Id.*

[68]Statement of Richard L. Skinner, Inspector General, Department of Homeland Security, Before the Committee on Homeland Security, U.S. House of Representatives (June 16, 2010).

[69]The existence of the Perfect Citizen program was disclosed in Siobhan Gorman, "U.S. Plans Cyber Shield for Utilities, Companies," Wall St. J. (July 8, 2010).

[70]NSA has denied aspects of the initial report. *See* "NSA Launches Infrastructure Cybersecurity Program," Information Week (July 9, 2010) [available at http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=225702741&cid=RSSfeed_IWK_News].

The result, beyond the perception of conflict, is confusion among the public and likely the creation of gaps and overlaps in authorities and responsibilities.[71]

III. RECOMMENDATIONS

Rationalize the Federal Structure

The current Administration has, through the appointment of a cyber coordinator, made a real effort to address the lack of cross-government coordination. But, as the recent GAO audit makes clear, there continues to be a confusion and overlap of responsibilities. The dry language of the GAO masks a traditional Washington concern—a battle over turf and budgets—and makes clear that more effort is required.

The outcome of this battle matters, profoundly. Authority follows responsibility, and who the Federal government charges with principal responsibility for cyber defense and resilience will determine whether our cyber response is primarily influenced by concerns grounded in intelligence or in network security. Our present plan, which divides responsibility for different domains among different agencies does not reflect the reality of the connectedness of the internet. It is all well and good to say that NSA and Cyber Command will defend the .mil networks, that DHS will bear responsibility for the .gov networks, and that the private sector will address problems in the .com and .edu domains. But the reality is that cyber traffic crosses domains; except for a few narrowed "walled garden" networks (like the government's classified networks), .gov and .mil traffic all travels through non-governmental nodes. Dividing responsibility for protection does not reflect the actual geography of the domain, which is precisely why the Department of Defense is aggressively planning to provide assistance through military capabilities to protect civilian networks.[72]

But the reality of current capabilities is such that no organizational plan is likely to succeed if a single federal agency is given a comprehensive lead responsibility. One would expect that sensitivities are too great to ever permit, for example, the NSA or CyberCommand to be responsible for protecting all parts of the Internet (though the Perfect Citizen program may well be an effort to do just that). Conversely, though it has the requisite statutory authority, DHS lacks the experience and expertise necessary to achieve results. What is required is decisive leadership from the White House to resolve the current confusion and provide a focal point for private sector coordination.

This is easier said than done. Precisely the same arguments were made in support of the creation of an Office of the Director of National Intelligence and in the creation of a Department of Homeland Security. In both cases a central focal point was thought necessary to achieve effective coordination of executive action. Both efforts may fairly be characterized as "ongoing works in progress" whose ultimate efficacy has yet to be conclusively determined. And just as the subordinated agencies have resisted inclusion within ODNI or DHS, it is likely (indeed nearly certain) that DoD and DHS would resist the strengthening of any White House control of cyber issues. It is highly likely any cabinet secretary will resist any organizational rules that constrain his or her ability to direct and control the personnel and resources within the Department.

There are two answers to this problem. One, reflected in the next section, is to have a strongly coordinated planning and policy development process at the White House/NSC level, so that disputes over implementation plans are minimized. The second, more controversial one is to recognize that the

[71]Emblematic of the challenges faced by the cyber coordinator is the recent memorandum allocating responsibility between OMB and DHS for federal agency compliance with the requirement of the Federal Information Security Act of 2002 (FISMA). *See* "Clarifying Cybersecurity Responsibilities and Activities," M-10-28 (July 6, 2010) [available at http://www.whitehouse.gov/omb/assets/memoranda_2010/m10-28.pdf]. Irrespective of the merits of that allocation, the memorandum is notable for the fact that it was co-signed by the cyber coordinator and the Director of OMB and issued on OMB letterhead, reflecting the coordinator's lack of directive authority.

[72]Lynn, "Defending a New Domain," at 104.

cyber domain requires giving directive, rather than coordinative, authority to an NSC-level official (who likely will require Senate confirmation and be subject to Congressional oversight).

This sort of change in organizational structure will be opposed by existing Cabinet members. It will require a strong commitment from the White House and a significant increase in the power of the cyber coordinator, and, no doubt, will necessitate legislative changes from Congress. To achieve a fully integrated cyber response, it would be necessary to give the coordinator authority to:

- Create a unified cyber security budget account within the President's annual budget submission and work with OMB and the NSC to set budget priorities with that account;
- Lead and coordinate the development of cyber security policy (including through chairmanship of the policy planning group described below, if that is created);
- Direct agency action in conformance with the budgetary and policy priorities set;
- Have dotted line authority over and a role in the selection of sub-cabinet cyber leaders (e.g. the commander of Cyber Command and the head of US-CERT); and
- Develop an enhanced set of objectives derived from the CNCI that will contain a set of measurable performance goals and objectives for cyber defense and resilience.[73]

To achieve this level of coordination and secure the cooperation of other federal agencies, it is almost certain that the cyber coordinator will need to, effectively, have cabinet-rank and report directly to the President. Any lesser degree of empowerment will, with near certainty, foreclose any realistic possibility of success. In short, if it wishes to advance the coordinative function in a meaningful way the White House must take ownership of the cybersecurity issue and work with Congress to endow the cyber coordinator position with the authority necessary to achieve a set of clearly defined and articulated goals.

The cyber coordinator will also have the difficult task of incorporating private-sector perspectives into the development of any Federal policy and in its implementation. Typically, Federal policy is informed by private sector views through the offices of the constituent cabinet agencies who participate in the policy development. Somewhat less frequently, private sector views are formally solicited through advisory committees and other less formal means of interaction. In the cyber domain, uniquely, Federal policies will have an impact on private sector equities and implementation issues will require private sector coordination. A critical task for the cyber coordinator will be the development of an effective mechanism for incorporating those view points.

Finally, it is worth acknowledging that we should not be completely sanguine at the prospects for success in achieving this sort of restructuring. In addition to opposition from agencies whose roles and responsibilities will be modified, we should anticipate significant opposition from both Congress and the regulated community. Congressional inertia and interest in protecting jurisdictional prerogatives[74] is widespread, as is regulatory resistance to any activity that empowers governmentalcontrol. Coordinated budgeting will require the cooperation of the Appropriations Committees in both houses of Congress in consolidating their consideration of the President's budget request. To the extent that legislative enactments are required to achieve centralizing objectives, their passage will require a significant investment of Presidential political capital.

Plan, Don't React

Instances of threat and response have been and, for the foreseeable future are likely to remain, subject to decision on a one-off, ad hoc basis within the context of working groups that create policy in reaction

[73]By way of analogy, Homeland Security Presidential Directive-5 designates the Secretary of Homeland Security as the principal federal official responsible for domestic incident management. Whether by statute or by executive order, similar (indeed greater) authorities could be afforded the cybersecurity coordinator.

[74]Witness the current divergence between competing cybersecurity bills proposed by the Senate's Commerce and Homeland Security committees.

to particular events. Thus, for the non-cyber responses to cyber threats, current structures appear to contemplate the development of alternative courses of action in a case-specific decision making process and not through a purpose-built decision making mechanism guided by an overarching policy. In such a situation choices among the various options (which can run the gamut of governmental responses) is likely to reflect as much existing capabilities as it is defined policy.

That sort of organizational structure and planning process does not do justice to the panoply of cyber attack and non-cyber response options. For purposes of a comprehensive cyber deterrence policy apparatus, the President should charter an NSC-led committee (notionally called the "Cyber Defense Options Group") whose initial task would be to survey and compile the potential modes for a whole-of-government response to a cyber intrusion or a cyber attack. Here, too, the cyber coordinator will need to find a mechanism for incorporating private sector perspectives.

Once this catalog of potential U.S. government actions is compiled, the response options should be subject to a rigorous risk-based analysis of consequence through red-teaming and other war game activities. In this way, the Federal government can create a menu list of possible responses that reflect a comprehensive range of potential activity and tie those potential responses to particular types of intrusions or attacks. The end result would be a coherent cyber deterrence policy that, in so far as possible, provides guidance in the anticipation of need.[75]

Maintain Human Control

The problem for cyber response is, in some ways, the same organizational challenge faced in other domains. The issue is "how to sustain human control [that is, maintain a] man-in-the-loop. . . . For example, control structures can have human control to unlock weapons systems, or automatic system unlock with human intervention required to override. An example of the former is the control of nuclear weapons and of the later, the control of a nuclear power reactor. This may be high tech, but the big questions are political and organizational."[76] Indeed, the problems associated with automated responses were demonstrated, in a more prosaic fashion, just recently when automated trading rules caused a 1000 point decline in the Dow Jones Industrial Average in less than 10 minutes of trading on the New York Stock Exchange.[77]

Our organizational structures and processes have not yet matured sufficiently in the cyber domain to understand this distinction, much less enable the implementation of policies that maximize the sustainment of human control at senior policy levels. To the contrary it would appear today that the default in response to a cyber attack is to permit critical decisions to be made at an operational level, informed only by system assurance necessity.

Such a structure is problematic. As an urgent matter, as part of the same options analysis recommended above, the Federal government should include within the ambit of the inter-agency study a charge to determine the means of maintaining policy level control of any cyber attack response to the maximum extent practicable. The governing rule should be, wherever possible, to "go slow" and permit human control. We have already seen how easy it is for automated systems to create a "flash crash;" we want to make sure that they don't start a "flash war."

And in those situations where a rapid response is deemed essential, default policies that must be implemented without human intervention should be identified in advance for consideration and human review. We should anticipate limiting these automated rapid response to essential defensive measures and affirmatively limit the extent to which offensive, aggressive measures are pre-authorized. The study group's proposals should, optimally, also be informed by consultation with the legislative branch.

[75]An important corollary benefit of the Cyber Defense Options Group would be to allow policy options to be developed with the input of those who would implement them, but not with their exclusive control. In general, the development of policy is best served when it is informed by but not subservient to the necessities of implementation.

[76]Tom Blau, "War and Technology in the Age of the Electron," Defense Security Review 94, 100 (London 1993).

[77]Nelson Schwartz & Louise Story, "When Machines Take Control," New York Times at B1 (May 7, 2010).

Create a True Public-Private Partnership

Engagement with the private sector has been only partially successful thus far. Many argue, correctly, that private sector information sharing networks exist at the technical level and are effective. But the reality is that we have yet to find a structure that enables strategic information sharing between the private sector and the federal government in an appropriate way.[78] Frequent reliance on cooperative councils, like the ISACs, has produced little more than the repetitive refrain that government can't share intelligence with the private sector and the private sector sees little to gain by sharing with the government.

Perhaps the time has come to consider a different organizational structure for cyber defense, for which the author offers this novel idea:[79] We might think about whether or not we should formalize the public-private partnership necessary for cyber defense by creating a Congressionally-charted, non-profit corporation (akin to the American Red Cross and the Millennium Challenge Corporation). One might notionally call it the "Cybersecurity Assurance Corporation" or "CAC."[80]

This potential organizational adaption would address many of the concerns that have frustrated the purely private or public responses. It would eliminate the "first mover" economic problem by federalizing the response. And it would allow greater maintenance of the security of classified information within the ambit of a government corporation. As a corollary, the quasi-public nature of the CAC might (if appropriate legal structures were adopted) provide a forum in which defense-related private sector information could be shared without fear of compromise or competitive disadvantage. Thus the CAC would provide a secure platform that allowed the government and the private sector to fully utilize our information assurance capabilities and call on both public and private resources.[81]

Indeed, the premise is that with the proper incentives private sectors actors can self-organize to achieve tasks.[82] It is simply the case that the current economic structures of cyber security do not provide those incentives. One significant benefit of the CAC structure would be to change the incentive structure to provide a secure, non-competitive forum where collaboration could be fostered.

At the same time, the quasi-private nature of the organization would provide greater assurance that legitimate concerns for privacy and government overreaching were suitably addressed. The centralization of the effort would allow for a unified and continuous audit of privacy compliance. The maintenance of a private sector control structure would further insulate against misuse and abuse by governmental authorities. And the absence of return on investment concerns would allow the organization to focus on privacy protection and network integrity.

Thus, a suitable organization would have some form of the following characteristics:

- *Board of Directors*—It is likely that an independent board would have appointees from government and the private sector. It might also possibly have non-governmental representatives from the privacy community;
- *Executive structure*—Any new corporation will require the full panoply of C-level managerial functions. At a minimum these will include a chief executive officer, and chief operations, finance, legal, and management officers;

[78]National Security Threats at 14.

[79]I am indebted to my former colleague at DHS, Adam Isles, whose thoughts on the idea of public-private partnership in a different context sparked this idea.

[80]This paper serves only as an outline of certain aspects of the CAC. The author acknowledges that significant further consideration and development of the idea are necessary, but offers these preliminary thoughts for the purpose of generating discussion. *See* Rosenzweig, "The Cyber Assurance Corporation," (forthcoming).

[81]Appropriate legal structures might include mandatory reporting; anonymization of information given to the CAC; compartmentalization of information that cannot be anonymized; and the development of a penalty structure for the misappropriation of CAC-protected information.

[82]*E.g.* DARPA Network Challenge (a/k/a Red Balloon Challenge), as described at https://networkchallenge.darpa.mil/default.aspx].

- *Security structure*—Given that the proposed CAC will be a repository for both classified information derived from government sources and confidential business information derived from private sector sources it will likely, itself, be the subject of both traditional espionage and cyber intrusions. A robust internal security structure will be essential;
- *Audit/privacy protective structure*—The critical innovation of the CAC is the creation of a unique structure that fosters the sharing of information. The principal goal of this structure is to assure transparency of operations while insulating the operations of the organization from political interference. Thus the most significant requirement (at least from the perspective of public acceptance) will be organizational structures that provide for a robust set of oversight mechanisms, including some sort of inspector general (IG)-like official with the responsibility for auditing compliance matters.

By far the most important requirement will be the drafting of an institutional charter clearly delineating the authorities and responsibilities of the CAC. What, after all, will the CAC actually do and how will it do it? At a minimum, one expects that the CAC will serve as a centralized information sharing system for threat information, much as the ISAC does now, but with a greater capacity to marry that information to government-derived data and, potentially, with the capacity to anonymize and re-distribute threat information more successfully than ISACs currently do. Indeed, the expectation is that, because of its particular authorities, the CAC will be able to achieve greater sharing than under current structures. If we judge that it cannot then the entire enterprise is not worth the effort.

In addition, the CAC should also be authorized to conduct the following additional functions: incident review and reporting; threat assessment and analysis; and the operation of intrusion detection and prevention systems. Of course, the devil is in the details: current owners of networks will be unwilling to delegate the responsibility for intrusion protection to the CAC unless they see a significant benefit from the collectivization of a security response. Again, if the CAC cannot achieve that objective the enterprise is without benefit. But, as this paper has argued earlier, the current model of complete reliance on private incentives to create the optimal level of intrusion detection and prevention has, plainly, not worked. The potential inherent in a CAC structure provides a half-way house that, if successful, will eliminate the natural instinct of the Federal government to fully federalize a response.

The initial charter will then need to identify the means by which the CAC can achieve its objectives. Will it have, for example, authority to define security standards and best security practices? Will it have regulatory authority to create and mandate private sector compliance? Will participation in its intrusion and detection activities be voluntary or mandatory? Will it be authorized to collect fees or reimburse expenses incurred by its private sector partners? And given the privacy sensitivities, under what rules will the CAC be authorized to cooperate with U.S. government authorities?

Many additional practical questions would, of course, need to be answered regarding the development of the CAC. Most notably the specifics of the governance structure of the organization will be critical. There will be detailed issues, including, for example:

- What qualifications are required for the Board of Directors?
- What would be the appointment/selection process?
- What degree of control would the Board have over the day-to-day executive leadership of the institution?
- Would anyone outside the board have a role in the appointment of executive level leaders?
- Would, as seems likely, the corporation be wholly private?
- Who would appoint the IG? To whom would the IG report?
- What powers of compulsion (if any) would the IG have?

One should not, of course, think that the creation of such a structure will be easy. It would require Congressional authorization, after all. Of equal significance, the start up costs of the CAC will require a

Congressional appropriation and the long-term funding needs will have to be addressed through some sort of fee mechanism. These are not modest challenges to the development of the CAC structure.[83]

Address Service and Non-Ownership Vulnerabilities

Finally, we need to give more concerted attention to the problems posed by the insecurity of our supply chain. Our current system (which, in a very limited way, reviews threats to our supply chain in some situations where a foreign entity takes corporate control of a critical systems manufacturer) plainly does not serve (and was not intended to serve) so broad a purpose. It is safe to say that under the current CNCI initiatives the U.S. government is still in the "information gathering stage" as it seeks to assess the scope of the problem and devise a workable set of solutions.

Recent recommendations for addressing the COTS problem reflect the difficulties that face us in devising a comprehensive solution. As the Defense Science Board recognized (and, indeed, recommended) the U.S. government will continue to purchase commercial goods for use.[84] It simply is untenable to suppose that the United States will ever forgo the economic benefits of a globalized purchasing system. Yet such a system inherently carries with it the risks associated with the off-shore production of goods and services critical to an infrastructure.

But strategies to eliminate the risk are non-existent and those required to mitigate it seem to be mostly nibbling around the edges. The Defense Science Board, for example, recommends:

- Increased intelligence efforts to understand adversarial intentions;
- Allocation of assurance resources on a prioritized bases to mission's whose failure would have the greatest impact;
- Better quality DoD software (to make malicious attacks more readily observable);
- Development of better assurance tools and programs;
- Better knowledge of suppliers processes and trustworthiness; and
- A robust research agenda.[85]

Likewise, the Department of Commerce, Office of Technology Evaluation, recommends relatively modest steps:

- Creation of a centralized counterfeit reporting database;
- Clarification of the Federal Acquisition Regulations to allow a "best value" purchase of IT components;
- Federal guidance to industry on the scope of criminal and civil liability for dealing with counterfeits and responsibility for reporting to the federal government;
- Broader law enforcement investigations of counterfeit activities;
- Federal leadership in disseminating best practices to industry;
- International agreements to limit the flow of counterfeit technology; and
- Better lifecycle planning to reduce the need to rely on problematic and unreliable vendors.[86]

The reality, however, is that steps such as these will not eliminate the risk to cyber assurance posed by the use of commercial systems. The dispersed nature of the cyber domain only serves to exacerbate the international character of the problem and render it seemingly insoluble. To supplement the ongoing CNCI Task 11 initiatives, the government should charter a broad-based study program (perhaps through

[83]One final note: It may well be that to foster some quasi-competition we might wish to charter more than one CAC.
[84]Defense Science Board, "Foreign Influence," at 51.
[85]Defense Science Board, "Foreign Influence," at 51-68.
[86]Department of Commerce, "Defense Industrial Base," at 208-211.

the National Academies) focused exclusively on the problem of COTS and supply chain security. Developing a comprehensive risk mitigation plan is both essential and, likely the best that can be achieved.[87]

As the government's examination of the COTS issue moves forward, the author offers two suggestions for additional steps that do not, thus far, appear to have been actively considered:

- We should consider expanding governmental review authorities to include situations where foreign entities take control of service activities that affect the cyber domain, or where foreign influence is achieved without purchasing full control (as in, say, a lease arrangement). Neither of these situations falls within the current domain of CFIUS or Team Telecom—yet the threat is no different whether Cisco's router production system is purchased by a foreign entity or all service for the routers is provided by that same foreign entity;
- We should also consider actions that would diversify the types of hardware and software systems that are used within the cyber domain. Such a diversification would, in effect, create a "herd immunity" against attack by malicious actors through both software and hardware intrusions.[88] For federal actors (and other governmental actors) creating herd immunity might be as simple as changing the Federal Acquisition Regulations to require product purchasing diversity. For private sector actors the government might achieve the same result by more vigorously enforcing the antitrust laws.

The author recognizes that both these suggestions are moderately controversial. Yet it seems self-evident that in the absence of concerted action the potential vulnerability posed by the reliance on COTS will not be alleviated.

CONCLUSION

As noted at the outset, any effort to identify optimal governmental structures and processes for cyber deterrence ought, in the long run, to be informed by the underlying deterrence policies adopted. Form should, in the end, follow function, not lead it.

That having been said, it seems clear that at this juncture our governing structures are not yet well developed and do not facilitate the adoption of coherent policies, much less permit their successful implementation. To a very real degree our failure to adopt a rational structure is a reflection of the medium with which we are dealing. The cyber domain is a non-hierarchical interconnected web of systems; we should be little surprised that our efforts to impose a hierarchical system of order on a fundamentally disordered structure have, to date, met with less than complete success.

But that does not mean that we should not try. Indeed, despite the difficulty, we must. If we are to maintain the utility of the web as a tool of communication and control we necessarily must adopt some form of hierarchy to protect the cyber domain. Whatever the policy chosen, clearer lines of authority within the Federal government and a more coherent structure of public-private interaction are necessary to allow for effective action. In sum that structure must:

- Provide for greater and more effective control of the Federal effort;
- Assure political control of any cyber response;
- Provide a means that will effectively allow for a public-private collaboration; and
- Find some means of providing for supply chain security.

The task, though simply stated, is a daunting one.

---

[87]Department of Commerce, "Defense Industrial Base," at 211.

[88]The author pretends no expertise in the epidemiology of herd immunity. What little understanding he possesses comes from a few useful review articles. *E.g.* P. Fine, "Herd immunity: history, theory, practice" 15(2) *Epidemiol Rev* 265–302 (1993). Notably, adoption of this approach is consistent with recent conceptual thinking suggesting that cybersecurity issues are analytically akin to public health problems. *E.g.* IBM, Meeting the Cybersecurity Challenge: Empowering Stakeholders and Ensuring Coordination at 11-23 (Feb. 2010); K.A. Taipale, Cyberdeterrence (Jan. 2009) [available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045].