National Security Threats in Cyberspace

Workshop Report
September 2009

American Bar Association Standing Committee on Law and National Security

National Strategy Forum

McCormick Foundation

American Bar Association Standing Committee on Law and National Security

The Standing Committee on Law and National Security, since 1962, has sustained an unwavering commitment to educating the Bar and the public on the importance of the rule of law in preserving the freedoms of democracy and our national security. Founded by five farsighted individuals, among them were Chicago lawyer Morris I. Leibman and then-ABA President and later Supreme Court Justice Lewis J. Powell, the Standing Committee focuses on legal aspects of national security with particular attention in recent years to the issues raised by legal responses to terrorist events. The Committee conducts studies, sponsors programs and conferences, and administers working groups on law and national security-related issues. Activities assist policymakers, educate lawyers, the media and the public, and enable the Committee to make recommendations to the ABA. It is assisted by an Advisory Committee, Counselors to the Committee, and liaisons from ABA entities. For more information, visit www.abanet.org/natsecurity.

The National Strategy Forum

Since 1983, the National Strategy Forum, a non-profit, non-partisan think tank in Chicago, Illinois, has focused on the issues and trends affecting US national security strategy. The NSF's principal mission is to enhance the public's understanding of national security-related topics through a monthly lecture series and the National Strategy Forum Review, a thematic quarterly journal. In addition to its public education programs, the NSF also conducts conferences on various subjects related to national security, including homeland defense, counterterrorism, nuclear non-proliferation, catastrophe preparedness and response, and international relations. Post-conference reports, issues of the National Strategy Forum Review, and more are available at www.NationalStrategy.com.

Workshop Underwritten By McCormick Foundation

The McCormick Foundation is a nonprofit organization committed to making life better for our children, communities and country. Through its charitable grantmaking programs, Cantigny Park and Golf, Cantigny First Division Foundation and the McCormick Freedom Museum, the Foundation positively impacts people's lives and stays true to its mission of advancing the ideals of a free, democratic society. The Foundation is an independent nonprofit. For more information, please visit www.McCormickFoundation.org.

Report written by Paul Rosenzweig.

Printed Courtesy of the HALO Corporation
ISBN 1-60442-631-4

The "National Security Threats in Cyberspace" Workshop was not for attribution.

National Security Threats in Cyberspace

June 4-6, 2009

Annapolis, Maryland

Table of Contents

Introduction

The last few years have seen a remarkable surge in the degree of concern publicly expressed by government officials regarding "national security threats" in cyberspace. The Bush Administration began development of a Comprehensive National Cybersecurity Initiative (CNCI) in January 2008[1]. The Obama Administration has followed with a Cyberspace Policy Review and a promise to appoint a "Cyber Czar" to coordinate a federal government response[2]. Funding for initiatives to protect the cyber domain is likely to increase significantly.

The ferment of ideas is substantial, even by Washington "crisis" standards. Some question whether a threat exists at all while others deem the threat existential. Novel issues of policy and law surface on an almost daily basis as technological innovation runs headlong forward, leaving policy-makers and concerned legislators trailing in its wake.

As the United States continues the development of its cybersecurity policy, the time is ripe for reflection and an examination of first principles. To that end the American Bar Association Standing Committee on Law and National Security, the McCormick Foundation, and the National Strategy Forum sponsored a two-day workshop in Annapolis, Maryland on June 4-5, 2009. The workshop brought together more than two dozen experts with diverse backgrounds: physicists; telecommunications executives; Silicon Valley entrepreneurs; Federal law enforcement, military, homeland security, and intelligence officials; Congressional staffers; and civil liberties advocates. For those two days they engaged in an open-ended discussion of cyber policy as it relates to national security. The discussion was under Chatham House Rules – their comments were for the public record, but they were not for attribution.

The workshop report you are now reading is the result of that discussion[3]

---

1. The initiative was announced in National Security Presidential Directive 54/Homeland Security Presidential Directive 23 on January 8, 2008. Much of the directive remains classified.

2. Cyber Space Policy Review (May 29, 2009) (available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf)

3. It should go without saying that the workshop did not produce a consensus on all issues. This report, therefore, is intended as a summary and should not be taken as reflecting the views of any individual participant, of the ABA, or the National Strategy Forum. Indeed, there are doubtless aspects of this report with which the various participants all individually disagree and they are not responsible for its content.

Working Group Members:

Stewart Baker
Partner
Steptoe & Johnson, LLP

M.E. "Spike" Bowman
Distinguished Fellow
University of Virginia
School of Law

Richard E. Friedman
President and Chair
National Strategy Forum

Al Harvey
Advisory Committee Chair
Advisory Committee on
Law and National Security

Jessica Herrera-Flanigan
Partner
Monument Policy Group,
LLC

Harvey Rishikof
Chair
Standing Committee on Law
and National Security

Suzanne Spaulding
Principal
Bingham Consulting Group
Bingham McCutchen, LLP

Lee Zeichner
President
ZRA LLC

Chapter I
What Are the National Security Threats Posed by Actors in Cyberspace?

Cybersecurity[1] threats are not synonymous with national security threats. Some cyberthreats do not threaten national security and, to be sure, any number of national security threats exist outside the confines of cyberspace. The workshop focused on the intersection of those two – on national security threats posed by actors in cyberspace. It sought to examine a wide array of threats in the virtual environment in cyberspace.

The Nature of Cyberspace – The threats arising from actions in cyberspace bear at least three characteristics – they are broad, embedded, and diverse.

First, the nature of the strategic threat in cyberspace is as broad as cyberspace itself. Any aspect of the world that is dependent on the cyber domain is at least potentially at risk. Thus, we are concerned with any adverse actions that might: threaten the integrity of our critical infrastructure; destabilize our financial system; allow the theft of intellectual property (where we conceive of intellectual property broadly to mean both commercially exploitable trade secrets and nationally significant classified information); or in any other significant way undermine our ability to rely upon technology for important national security objectives.

Second, threats to the integrity of information and security in cyberspace are deeply embedded in the cyber domain. They arise both from potential vulnerabilities inherent or placed in complex software operating systems and from potentially malicious hardware. We characterize the problem as embedded since the potential threat is an intrinsic feature of cyberspace and therefore can never be fully eradicated.

Third, the threat in cyberspace is diverse. It is characterized by a plethora of potential malefide actors. The cyber world is populated with more than nation-state actors: there are also well-organized criminal gangs; independent terrorist organizations; and "just for fun" hackers of every stripe on the stage. Each poses a distinct sort of threat, requiring a nuanced differential response.

Most workshop participants were of the view that the nature of cyberspace there-

[1] A Note on Usage: As Strunk & White note in "The Elements of Style," the "steady evolution of language seems to favor union" of compound words – from "cyber space" to "cyber-space" and then finally to "cyberspace." We are in the midst of that linguistic evolution for the cyber domain. Our usage throughout is consistent with what we understand to be common usage generally and, where feasible, with the usage in the President's Cyber Space Policy Review, supra.

fore made threats from that domain fundamentally different in nature from those existing in the "real world." Several factors contribute to this difference:

• The span of cyberspace is global in nature, creating conflicting and overlapping realms of control by nation-state actors with differing legal and cultural approaches and distinct strategic interests.

• We have become sufficiently dependent upon the cyber domain for communication and control of the physical world that disassociation is effectively impossible. Cyber globalization cannot be undone. This is especially true given our increased reliance on cyberspace for national security functions.

• Globalized production of both cyber hardware and software (e.g. in China, India and Mexico) makes it virtually impossible to provide either supply chain or product assurance.

• The scalability of the cyber domain makes it qualitatively different. We are not dealing with a kinetic force (like a bomb) which even in the most extreme circumstances has a physically limited range, but with the mechanism by which we communicate and control real world operations on a global scale.

• Like many other specialized fields of knowledge, operations within the domain are controlled by a relatively small number of people. Everyday users do not have the practical ability to modify or control the software and hardware that they use. Put more bluntly, a small number of people effectively control, or can manipulate the cyber universe.

• Paradoxically, despite the concentration of specialized knowledge required, the distributed nature of the cyber domain prevents any one single person or group from exercising complete control. Because of the interconnectedness and interoperability of cyberspace, no locus of positive control is feasible. Efforts to mitigate the threat (to the extent doing so is possible at all) will require international coordination.

• Changes in the cyber domain occur with great rapidity, based on ever advancing computational and communications technology. The interconnectedness of cyberspace enhances this consequence of acceleration. Vexingly, each change creates a new cycle of vulnerability and response. Far from being static, cyberspace is almost overwhelmingly dynamic.

• The distribution of cyber assets spans all types of organizations, from closed systems and governmentally controlled ones to systems owned and operated by

non-profit and profit-making members of the public, each with different resources, capabilities and concerns.

• And, finally, the nature of cyberspace is such that we currently lack the technical capacity to attribute actions to the responsible actors with a high degree of confidence. Though identity may sometimes be inferentially determined, the process is difficult and practical anonymity is achievable.

A consequence of the unique structure of cyberspace is that fundamental precepts that work in the physical world – precepts of risk management and deterrence – have less ready application in the virtual world.

First, common risk management mechanisms will not work as effectively as they do in the physical world. Often, risk management involves systems for the detection, avoidance and mitigation of risk. In the globalized cyberspace these efforts to detect and monitor threats are sometimes technologically unfeasible. Even when feasible, elimination of risk is often impractical because the risks are systemic and resistant to traditional cost-benefit analysis. In a world where the identity of the threat cannot be determined with confidence, mitigation of that threat is problematic. Moreover, traditional models of deterrence, which rely on the identification and punishment of malefide actors, cannot operate as readily in this environment.

More saliently, even to the extent that traditional risk management practices are effective, they represent a direct and significant cost to the system. Each layer of security to prevent unwarranted intrusions is also a potential barrier to the efficient operation of a cybersystem – security always creates a cost of some sort, and that cost will need to be borne by some actor in the system.

Thus, one must recognize that the collective cost of the existing vulnerabilities paid by society is very large. All of the protective measures we take today (firewalls, monitoring systems, audits, etc.) are, effectively, transaction costs that add nothing productive to the system. Likewise, the social costs that remain from the vulnerabilities that are not resolved are daunting[2].

[2] It is also true, as some participants noted, that every vulnerability is also an opportunity – both an opportunity, when identified, for proactive action by a system owner to protect the system and also, in some instances, an operational opportunity for our own government in appropriate and lawful circumstances.

As a result, one strain of thought is that we will need to learn to live with a system that tolerates a certain amount of insecurity – threats are both impossible to eradicate and costly to do so even to the extent possible. Hence at least one part of an approach to security is to build systems that are able to operate under the assumption that security breaches will occur and that the "bad guy will get inside." This suggests a strong emphasis on system architectures that employ multiple tiers of defenses, can be segmented when under attack, and have a healthy component of resiliency to allow speedy recovery.

Indeed, all of the participants were generally of the view that the system vulnerabilities were inherent in the current structure of cyber systems. Concerns were expressed about the perception that market forces are driving delivery of products that are not meeting customer security needs. The IT industry needs to change and the consumer needs to realize that products provided are, effectively, the root of the problem. Product cycle time is driving the market and the cost of the insecurity that arises from the rush to delivery is distorting it – a situation that is simply "chaotic." And, absent a fundamental restructuring of current security methodologies, the use of monitoring to act as a preventative measure, while an understandable response, is likely ineffective. This Maginot Line mentality is, for a host of reasons, an inadequate response.

Virtual Worlds; Virtual Threats? – After examining the intersection of the cyberworld with the physical or kinetic world, the workshop also considered another novel phenomenon – the development of seemingly independent virtual realities where real-world actors can interact on-line in created worlds. These include sophisticated games, like World of Warcraft and systems that mimic the real world, complete with economic and social interactions, such as Second Life. These worlds are distinct from traditional cybersystems and in many ways defy our ability to monitor actions that occur in them. The simplest of these virtual worlds (MySpace and Facebook) would, if they were real-world populations, be the 11th and 6th largest nation-states, respectively. Some of the more complex systems are also growing impressively large – Maple Story[3] has over 92 million users.

Of equal note, some of these second worlds are designed with deliberate real-world connections. Thus, for example, consider the mixed reality world (linking the real world and the virtual) that the government creates for its own benefit

[3] Maple Story is a MMORPG (massively multiplayer online role-playing game) where the players take on powers as warriors, magicians, thieves, or the like and interact with each other while performing tasks within the virtual world. See http://www.maplestory.com/

when it uses virtualization to control Predators in the Afghanistan/Pakistan region whose real-world consequences are quite deadly. If only for its use as a kinetic force-projection mechanism, the virtual world is one of critical national security interest.

Indeed, given the degree to which virtual worlds seek to simulate the real world, we should not be surprised that we face all the same sorts of potential for criminal or other malevolent behavior in these second environments. Already we see sophisticated securities frauds that have virtual world consequences. Second Life has, reportedly, had its first instance of bank fraud. EVE Online, another social interaction construct, has had several well publicized bank frauds. And China has legislated government control over virtual currencies in response to virtual world operators issuing their own currencies and allowing them to be used in the "real world."[4]

But the challenges of the virtual world are most relevant when they overlap into the physical world. The interactive nature of the virtual world makes it an ideal place for "spear-fishing" – using an official-looking request to secure personal information – increasing the likelihood that individuals will be unwittingly recruited to act against their own interests or, depending on what they disclose, the interests of their country, company or organization.

Thus, the nature of the virtual world risk arises from a systematically greater inability to control information. In the virtual world (even more than the physical one) the distinction between operational information and data security is disappearing. This will have the real-world consequence of making us vulnerable to attacks on information systems and things we operate. The difference, one should hasten to add, is not one of kind but of degree – the virtual world fosters a "degradation" of security.

Other risks arise from other interactions between the virtual world and real-world events. National security threats may arise, for example, when digital virtual currencies are traded in a virtual world in a manner that effectuates the real world transfer of funds for purposes of money-laundering. It is, in effect, an unregulat-

[4] See Real Taxes for Real Money Made by Online Game Players, Wall St. J. (Oct. 31, 2008) (available at http://blogs.wsj.com/chinajournal/2008/10/31/real-taxes-for-real-money-made-by-online-game-players/).

ed system of exchange (much like the Hawalas [5] are in the real world). Because the core of most virtual worlds is a real functioning "economy" (even if only offering trade in digital magical weapons), the situation is ripe for manipulation of the system. This is particularly the case since very little "real world law" applies directly in the virtual world (beyond, perhaps, the confines of contractual agreements between the users and the providers) and any application of "real world law" is fraught with challenges.[6]

In short, the growth of participation in virtual worlds has not created any new and different national security threats, but it has clearly enhanced the capacity to commit real-world "crime" already and may augment the capacity to commit real-world terror.[7]

Attribution – Who are the Threat Actors? – The introduction to this issue would be incomplete without a return to the vexing topic of attribution. We see threats of various flavors in many dimensions. We can readily imagine attacks of significant consequence. This raises vital questions of policy and doctrine – if a cyber attack took down our financial system, would the United States consider it an act of war? If so, how would we know against whom to strike back?

This question – identifying *who* the attacker is – is exceedingly different in the cyberworld than in the real world. To be sure, in the physical world that is sometime a challenge. But forensic capabilities in physical space are far more advanced than they are in the cyberworld.

We know, for example, that cyber attacks against Estonian government services, financial enterprises, and media outlets in 2007 were sufficient to cause NATO to develop and approve a new cyber defense policy; and attacks did occur against

[5] Hawalas are part of an informal banking system common in many parts of the Arabic culture. Tied by links of family and kinship, hawaladars (individual bankers) will extend credit or make payments locally based upon communications with their partners overseas. With the flow of debts and obligations back and forth, actually settlement of debts between individual hawaladars is relatively infrequent.

[6] In addition to China's recent move to regulate virtual currency, South Korea has a body of case law that applies to virtual activity. Applications of American law to the virtual word are sporadic and, as the MySpace suicide case discussed below makes clear, fraught with difficulty.

[7] One interesting research project identified would be to examine the parallels between the emergence of virtual currencies in the virtual world and the emergence of new mediums of exchange in the real world (e.g., the creation of the Euro zone, the use of Special Drawing Rights (SDRs) as a substitute world currency, or the creation of a market in cell phone minutes in developing coutries). Participants were intrigued by the possible parallels (and the possible distinctions).

government computers in Georgia during its conflict with Russia.[8] Though one suspects governmental involvement in these attacks, that supposition is at this juncture unproveable.

Likewise, consider the GhostNet system recently evaluated by a Canadian information security group.[9] The GhostNet involved a sophisticated infiltration of many computers used by governments and non-governmental organizations who had diplomatic contacts with China. Indian embassies were infected as were the Dali Lama's information systems. Through sophisticated counter-hacking, the Canadians were able to trace the cybersignal back to control systems in Hainan, China (perhaps coincidentally, the home of a Chinese signals intelligence facility). But they could go no further.

Consider then, as we close this chapter, the simple question – is that enough? If a cyber attack traceable to Hainan had, say, shut down an American electric grid in the Midwest, what would be the response? What degree of confidence in the conclusion would be high enough? How does the fact that the grid is mostly in private hands effect the analysis? What about other, less critical pieces of infrastructure?

These questions make clear that we are becoming dangerously reliant on our IT technology. They also make clear that cyber policy and doctrine have yet to be well-developed. The following chapters offer one set of views on how we have responded so far, and how we should respond going forward.

---

[8] Though no clear evidence exists attributing these attacks to Russian state actors, both Estonia (Estonia Accuses Russia of Cyberattack, Christian Science Monitor (May 17. 2007) (available at http://www.csmonitor.com/2007/0517/p99s01-duts.html)) and Georgia (Report: Russian Hacker Forums Fueled Georgian Cyberattack, Wa. Post (Oct. 16, 2008) (available at http://voices.washingtonpost.com/securityfix/2008/10/report_russian_hacker_forums_f.html) have contended that Russian influenced hackers were the cause of the attacks. The NATO Cyberdefense Center of Excellence was opened in Tallinn, Estonia in May 2008.

[9] 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)

Chapter 2
How Are We Addressing Threats in Cyberspace?

Aristotle said, "If you would understand anything, observe its beginning and its development." The history of responding to threats in cyberspace is relatively brief, but its progeny is ever changing.

Twenty-five years ago, the concept of cyberspace and cyberthreats was barely a twinkle in the eye of a few academics and theorists. In 1988, when Robert Tappan Morris released the first computer worm onto the Internet, it was an oddity and an experiment gone wrong.[1] Indeed, the Morris worm prompted DARPA to fund the establishment of the Computer Emergency Response Team Coordination Center (CERT/CC) at Carnegie Mellon University to give experts a central point for coordinating responses to network emergencies – quite possibly the first institutional structure developed for cyberthreats.

Today, the nature and scope of institutions responsible for responding to cyberthreats are as broad and diverse as the threats themselves. They range from governmental structures to private organizations to aspects of the private market. There are, as one might expect in a rapidly changing world, many gaps and overlaps. But any effort to address cyberthreats comprehensively must begin with some baseline catalog of where we are today.

Governmental Responses – The governmental response to the cyberthreat has taken primarily two tacks – one legal and one organizational. Neither has been very well unified or coherent; rather, they have been more organic in their development and, consequently, less cohesive than we would wish.

The legal effort began, for all intents and purposes, in 1986 with the Computer Fraud and Abuse Act (CFAA) which criminalized limited forms of computer crime.[2] For the most part, as described more fully in the next chapter, our legal response domestically has been fairly effective in criminalizing malfeasant behavior. We've expanded substantive criminal law where necessary and applied existing laws (against fraud and extortion for example) in the new cyber domain with relatively modest doctrinal difficulty.

Thus, the famous MySpace suicide case (in which charges were recently dis-

[1] See United States v. Morris, 928 F.2d 504 (2d Cir. 1991).

[2] Currently codified (as amended) at 18 U.S.C. §1030.

missed) was really about suicide, not cybercrime.[3] To be sure, it raised interesting issues of criminal law and causation, but the cyber-related issues of using MySpace as a means of causing harm did not change the fundamental nature of the crime.

Rather, as detailed more fully below, the single greatest difficulty encountered thus far in the development of a legal response lies in the transnational nature of cyberspace and the need to secure international agreement for broadly applicable laws controlling offenses in cyberspace. Traditionally law is viewed as territorial and criminal law is concerned with controlling crime. Prosaically, countries ask why they should care if citizens are conducting crimes outside of their country.

To be sure, we do have extradition laws that may be applied, but they typically require that both nations deem the acts in question a criminal offense –but not all nations recognize cybercrimes. Moreover, many cyber events are truly multinational in nature (botnets, for example, are automated collections of compromised computers that act as "robots" and use systems and nodes literally around the world) making effective extradition impractical. The capacity to act transnationally and to conceal identity in cyberspace creates qualitative distinctions that make all the legal difference.

The organizational governmental response was slower to develop and has proven even more diffuse. After the creation of CERT/CC by DARPA the next significant step occurred in 1996 with the creation of a presidential critical infrastructure board. Later President Clinton issued Presidential Decision Directive 63 which reflected the first comprehensive attempt to set out the structure of how the US was going to protect its critical infrastructure (both physical and cyber) from attack.[4] Since then we've seen a continuous series of structural reorganizations. The Homeland Security Act led to a restructuring that moved many cybersecurity components to the Department of Homeland Security. In 2007 President Bush announced a Comprehensive National Cybersecurity Initiative which heralded

---

[3] Lori Drew (age 50) was initially convicted of misdemeanor offenses relating to her cyberbullying scheme against 13-year-old Megan Meier. The scheme played a role in Meier's suicide. The district judge subsequently threw out the conviction which was based on the novel argument that Drew's bullying violated the MySpace terms of service. See Kim Zetter, Judge Acquits Lori Drew in Cyberbullying Case, Overrules Jury, Wired (July 2, 2009) (available at http://www.wired.com/threatlevel/2009/07/drew_court/)

[4] Critical Infrastructure Protection, Presidential Decision Directive 63 (May 22, 1998) (available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm)

a coordinated government response. And earlier this year, President Obama announced the results of his own cybersecurity review. There has been, to be blunt, no shortage of organizational responses.

From our perspective, the key national security problem with our governmental response has not been lack of awareness. Rather, many workshop participants thought that lack of leadership and stability are the main factors limiting our capacity to respond. To this some would add the concern that there have not been a large number of people working in the field of cybersecurity who also have a national security background. Cyberspace has gone from being an ornament of interest to forming a real pillar in national security efforts. But in doing so, the lack of expertise has led to confusion in defining the core issues that our governmental organizations should address.

What, fundamentally, defines a national security problem? Clearly, the concept encompasses a threat that would affect our military capability and our security in a way that gives the opponent an advantage. We also consider that counterintelligence problems within cybersecurity (relating to the integrity of software and hardware) are, from a governmental perspective, the most significant problem today. Vulnerabilities both render our nation's secrets subject to exploitation and, even more frequently, permit foreign governments and affiliated groups to conduct cyberindustrial espionage. And yet we perceive that a comparatively limited amount of resources are being devoted to the counterintelligence function.

The situation is not aided by the episodic attention paid to cyber issues by Congress. There has been insufficient continuity in handling cybersecurity issues in the legislature which addresses the question only in fits and starts. The Y2K episode is the best known example of this phenomenon.[5] Congress was concerned and then the problem was, seemingly, resolved, with a subsequent loss of legislative attention. The current growth in cybersecurity concern has produced a number of recent hearings and some members are interested in the subject, but

[5] Y2K is shorthand for the fear that significant disruptions would result from the failure of early computer programs to account for the digit change from 1999 to 2000 in their software.

the challenge will be to sustain that interest and turn it into effective action.[6]

Yet if Congress is to be faithful to the Framers' vision of its role in the nation's defense, it must exert itself. There is little doubt that if it does so, it can (and should) play a significant part in the development of policies for conflict on a digital battlefield. Indeed, as we have seen since 9/11, it is essential that Congress play a role in enacting rules to ensure that American counterterrorism policies are carried out. It will be especially important that Congress address critical organizational issues regarding the allocation of responsibility within the Executive Branch.[7]

Private Sector Responses – If the government response can be characterized as ad hoc, the private sector response can best be characterized as unstructured. And if a threat to our military strength is a national security threat, then (as the Romans believed) it is equally true that a significant threat to our economic strength is a national security threat as well – a reality that makes the lack of a coherent private sector response all the more problematic.

For one thing, private sector security is often governmental security. Our communications frequently use public systems, for example. The electrical sector is, likewise, a critical area on which both the private sector and government are dependent. The overlap of vulnerabilities is striking.

But creating incentives for security in the private sector cyber domain is a challenge. Workshop participants agreed that by and large the question of security vulnerabilities was caused by a systematic market failure. The costs of security failures often are not internalized by private sector actors (this is, obviously, not always the case – costs sometimes fall on the actors themselves) in a way that incentivizes them to take adequate protective steps. In this way, security for the broader system of the entire Internet is a classic market externality whose true costs are not adequately recognized in the prices charged and costs experienced

---

[6] Recent hearings include: Cybersecurity — Assessing Our Vulnerabilities and Developing An Effective Defense, Senate Committee on Commerce, Science and Transportation (March 19, 2009); Cyber Security, House Permanent Select Committee on Intelligence (Sept. 18, 2008); Implications of Cyber Vulnerabilities on the Resilience and Security of the Electric Grid, House Committee on Homeland Security (May 21, 2008); The Cyber Initiative, House Committee on Homeland Security (February 28, 2008).

[7] See Stephen Dycus, Congress's Role in Cyber Warfare, 3 J. Nat'l. Sec. L & Plcy. __ (2009) (forthcoming)

by individual actors. Indeed, one participant, rather unkindly, characterized the private sector response as a "faith-based market failure" – one bottomed on an act of faith that vulnerabilities would not be exploited. That faith has, of course, gone unrequited.

There are three traditional responses to market failures of this sort – regulation, taxation, and insurance pricing. None of these functions as well as we might wish in the cyber domain.

Taking the last of these first, insurance pricing is not feasible without both standards against which to measure conduct and liability that arises from failure to meet those standards. In the cyber domain, neither is readily available – there are no generally accepted cybersecurity standards and there is no generally applicable liability system in place to account for failures to meet those standards.[8] The relevant insurance question is: how do you underwrite the risk? And the answer only can come if the risk taker is motivated by liability to insure the risk in the first place, allowing its collectivization. Right now that system simply doesn't exist.

In thinking about this question one must recognize that the issue of liability is one of those political "third rails." For a host of reasons, private sector companies are unwilling to publicly identify security risks and equally unwilling to voluntarily create standards that lead to liability where none currently exist. If the government doesn't step in to set standards for private sector to follow, then none are likely to be developed. But the construct of a government-developed set of standards is itself fraught with challenges – not the least of which is government's chronic inability to conduct itself like a profit-making organization.

In short, to have an insurance and liability system, you need metrics of performance. Government is not hopeless in this regard – fire codes and building codes form the foundation of insurance today. But until attribution systems are more widely developed and applied and performance metrics more commonly agreed upon, liability (and insurance against liability) responses will be unavailable. One alternative, worthy of consideration, is to reverse the paradigm – instead of

[8] There is a liability standard increasingly applicable to a limited class of cybersecurity cases in which the data integrity of customer information is breached. See 15 U.S.C. § 6801 and 16 C.F.R. § 314.4(a)-(c). But this liability structure is not yet fully developed and applies to a problem – data and identity theft – which, while clearly troubling, may not rise to the level of a national security concern

government creating standards, the breach of which might result in liability, it ought to be more feasible for the government (in partnership with industry) to develop a set of recommended best practices for cybersecurity. If it did so, it is possible that an independent certification industry would develop and that insurance rates would follow compliance with those standards. Alternatively, though less efficiently, the government might, itself, give a "gold seal of approval" and certify compliance with the best practices standards. In either event, if standards could be developed, then insurance against the risk of breach of those standards would naturally follow.

A somewhat more intrusive step down the road would be to change from advisory standards to a traditional regulatory model of mandatory standards. This, too, would raise questions about government's ability to define the standards appropriately. It would also raise the routine problem of operationalizing regulatory mandates in a complex technical area. Even cyber-sophisticated governments like Estonia have been shut down because they did not know how to address threats and vulnerabilities and create doctrine about risk. How then are we to define crisp parameters to deal with these threats that could be mandated for the private sector?

It may be, however, that the regulatory model can be followed without any standard-setting. In this vision, all a government need do is define the desired outcome (e.g. appropriate reductions in "data breaches" or "intrusions") and define the penalties for failure. Simply creating consequences also creates liability (and thus insurable risk) even in the absence of a mandate on how to achieve the results desired. As long as the desired results expressed are not impossibilities (e.g. elimination of all intrusions) this would leave the private sector to determine the most cost-efficient means of achieving the public policy objective.

This discussion leads to the final means by which government can incentivize private sector activity – the tax code. If we tax an output or provide a tax credit/incentive for an expenditure we create a financial incentive to act – one that history has shown to be fairly powerful in its ability to shape behavior. Though many workshop participants believe that using the tax code to incentivize conduct can have unintended and undesirable consequences and that our record of using the tax code for incentives is poor, it nonetheless remains a tool by which our government has frequently sought to modify private actor conduct. In this case, for example, Congress might consider a tax credit for qualifying expenditures on security systems as a way of pushing the private sector towards more security-conscious decisions. This would, as noted, require some confidence in

the government's ability to craft the right incentives – a confidence that many workshop participants lacked.

And that is precisely the problem. Especially in the cyber domain where the private sector actors are notoriously distrustful of government interference and regulation, it will take a significant effort of political will to create the culture where civil law drives security reform. Prospects in the near term are, candidly, rather dim and finding a workable solution will pose a serious challenge for the new Cyber Czar.

Information Sharing – The difficulty of any regulatory approach or any approach with a strong governmental input can readily be seen in the challenges we face in the comparatively simple world of information sharing. One would think that identifying and communicating about new cyberthreat developments would be relatively simple to achieve. It is not.

Everyone purports to believe that we need more information sharing. But no consensus exists on precisely what that means, or whether it would truly be effective. What information needs to be shared by the government with the private sector and what from the private sector should be shared with the government? How would it make a difference? And of course, how will the recipient use the information?

There are huge disincentives to reporting cyber intrusions. If, for example, a bank in the financial community finds out that it has a vulnerability, then public disclosure of the fact will convert the vulnerability into a stock valuation problem. CEO's refrain from talking about cybersecurity problems because of perception issues, yet most of them know they are vulnerable. They are aware, metaphorically, that their "Hong Kong office" routinely is probed.

Several participants, however, disputed the notion that information sharing is limited. They acknowledged that antitrust laws created a barrier to some forms of sharing. They also agreed that the prospect that their confidential business information would be subject to public disclosure under the Freedom of Information Act (FOIA) if shared with the government created a barrier to information sharing that was difficult to surmount.

But they also contended that many private sector mechanisms for information sharing already existed without the need for government intervention. The pointed, for example, to the "white-hat hacker" or security researcher community,

which provides a valuable private sector service. Members of that community are active information sharers and even today head off a vast number of attacks and identify many vulnerabilities before harm occurs.

Moreover, some participants were of the view that, on a technical level, information sharing about vulnerabilities and remediation happens routinely in the private sector. This isn't because of a mandate from the federal government. Rather the impulse to share is based on a well-grounded exchange of network-protective information done at the technical level by the engineers of, for example, the major telecom companies. Under this view, there is little need for a government mandate to share. And, they contend, if the government wants to join in the sharing, they would be welcome – if they bring added value to the arrangement.

Industry will agree to sharing information only if doing so is "useful" by some metric of usefulness that they are willing to acknowledge. Their concern is threefold: first, they doubt that information shared with the government will actually help anyone; second, industry is anxious to avoid burdensome, costly, government mandates; and, finally, industry is concerned that information shared with the government might be used for purposes other than the security purpose that underlies the original request.

And they are also concerned that government-to-industry sharing is not of great value – what will industry get from government that will be useful in influencing its actions? Some participants thought that governmental sharing of threat signatures would be of great utility – others were less convinced.

Thus participants were of the view that we need to establish a new set of protocols for reporting vulnerabilities. They suggested thinking about information sharing in a different way. Some participants urged adoption of the concept of coming into a neutral space to exchange information which, at the end of the day, an entity takes away only for a specific purpose. As a recent study by the Center for Strategic and International Studies noted, this construct allows a group to come together to solve a problem, and ensures that identified information is shared so that the problem is solved.[9]

Imagine, for example, that a particular bank has been hit very hard by some form

[9] See Securing Cyberspace for the 44th Presidency (CSIS, Dec. 8, 2008) (available at http://csis.org/publication/securing-cyberspace-44th-presidency).

of cyber intrusion. The bank has every incentive to treat it as a non-event, yet there are global implications for market stability. We need a process in place to allow the bank to reach out to the intelligence community to deal with the challenge and to share information with other banks who might be affected. Rather than build a single location for all information sharing, the optimal result would take advantage of the internet's dynamic nature to create an information sharing space designed to solve a single specific problem that will disappear after the problem is addressed. This space might also be open to users (and not just system administrators) who will often have valuable insights into a problem.

As an added twist, workshop participants also considered the possibility of monetizing solutions, by creating a payment structure for the sharing of information that is of value to others – if a company were paid for disclosing its vulnerabilities and response that would surely change the information sharing dynamic.

Finally, we also need to emphasize that the flip side of sharing information for security purposes is often (or may be) a challenge to privacy. The cyber domain prizes its anonymity in a way that is the converse of the attribution problem. Similarly, it values the lack of governmental or private monitoring and intrusion in a way the conflicts with many developing security solutions. In focusing on the threats and vulnerabilities we do not mean to disregard the equally trenchant potential for governmental abuse. To a large degree participants thought that abuse could be ameliorated by greater transparency of governmental functions. But all recognized that at some fundamental level our cybersecurity measures could pose a challenge to our cherished liberties.[10]

*****

The governmental and private sector responses are not fully cohesive, and both have developed without a great deal of thought. Participants were of the view that we need a comprehensive, national, White House-led strategy – one that not only begins the public-private partnership discussion that needs to occur to unify our cyber response, but also one that uses the bully pulpit of publicity to generate awareness of the need for change.

[10] For this reason a number of workshop participants were especially skeptical of current government proposals to monitor government-bound internet traffic and nodes where private traffic also was present. In their view this nascent program, known as Einstein 3, raised significant concerns about privacy that were not adequately addressed in publicly available information about the program.

Chapter 3
Legal and Doctrinal Issues in Cyberspace

Our discussion so far has made clear that the threats in cyberspace are significant. They derive from the nature of the network – its interconnectedness, scale, speed, and the challenges of comprehending precisely what is happening in any particular instance. The problems are, in all likelihood, persistent and unlikely to change.

The question then is how the legal and doctrinal analysis should change to accommodate the new realities of cyberspace. Traditional causation-dependent and geographically bounded régimes are less likely to be of utility in cyberspace. The question then is how to adapt law and doctrine to the cyber domain.

Three distinct legal régimes are potentially applicable to the government's response to threats emanating from cyberspace: criminal law for law enforcement; international law, including the law of armed conflict, for war-like kinetic and cyber responses; and intelligence law for actions relating to covert actions and the collection and analysis of data about cyber adversaries.[1] The questions we ask are: Do we need more law? Or do we have enough legal authority to act now? And how does law control (or the lack of law limit) US government reaction to an ongoing crisis?

Criminal law – The application of criminal law to cybercrimes raises issues of substantive law, procedure, and forensics. While in the real world distinguishing a crime from an accident is relatively straightforward, the exercise is much less easy in cyberspace. In the end, this unique characteristic makes prosecuting cybercrime particularly difficult.

Substantively, though the law is still evolving, we have, for the most part, developed an adequate set of laws for offenses involving unauthorized intrusions into cybersystems. These intrusions diverge from traditional crime but can be readily analogized to more old-fashioned common law concepts like trespass. Steadily, laws have adapted to make clear that hacking intrusions are crimes in and of themselves, as is trespass, and we now are building an adequate legal system to deal with situations similar to the concerted denial of service attack on Estonian systems. If that event had occurred in the United States it likely would have been criminal under recently enacted laws.

---

[1] A fourth régime of civil law and liability will act independently from government intervention. Those laws (and the incentives they create for the private sector) were discussed in Chapter 2, above.

Criminal law has also adapted fairly readily to situations in which computer systems are not the object of the crime but are used as tools to commit crimes of a more traditional nature. Using computers to commit fraud or access child pornography does not involve any legally relevant distinctions from the use of note paper or the mails to commit the same offenses. In general, criminal law focuses on the illegal conduct itself and is suitably neutral as to the means by which the crime is committed. Some legislatures have perhaps gone too far beyond this construct and made it a crime to commit a particular offense (e.g. theft) using a computer – but in general that response seems unnecessary (in contrast, for example, to offenses that are rendered more serious through use of a weapon). Still, this expansion, while unnecessary, is little more than a distraction from the generally appropriate structure of criminal law.

In the criminal law context, then, substantive challenges are relatively modest. The same cannot be said of procedural issues. Most American procedural criminal law requirements are premised on the assumption that the crimes to be investigated and prosecuted have occurred within the geographic boundaries of the United States. In the rare cases where cybercrimes are geographically limited in this way, these procedural requirements are suitable. But the reality is that cybercrime is predominantly (and almost exclusively) transnational in character.

In many ways the situation is much like the challenge facing state law enforcement officials prosecuting Depression-era bank robberies. The perpetrators could escape investigation and prosecution simply by changing jurisdictions and hiding behind differing laws. The problem is best exemplified by Clyde Barrow's famous fan letter to the Ford automobile company, thanking it for providing the means by which he and Bonnie escaped justice.

The solution, of course, was to federalize the crime of bank robbery and, effectively, eliminate the boundary problem. But what the US government could do with the stroke of a pen takes, in the international context, years and years of work. Today we are just at the beginning of constructing a transnational set of procedural rules for cybercrime. For the most part, information sharing across national boundaries is slow and limited – far slower and more limited than the nimbleness with which criminals can change their tactics. Substantive convergence of the law is even further in the future and may well prove impossible.

To date the only successful effort to develop a unitary procedural approach to cybercrime is the Convention On Cybercrime developed by the Council of Europe. It aspires to create a single set of cyberlaws and procedures internationally

in order to insure that there is no safe harbor for cybercriminals. But the process is slow – only 26 countries have ratified the Treaty in eight years. And significant cultural and legal hurdles (e.g. differing American and European approaches to "hate" speech) have further slowed convergence. Thus in the criminal domain the single most significant question is one of extraterritoriality and engendering cooperation from international partners.

To the procedural challenges of criminal law, one must add a final piece – the significant forensic challenges of actually solving the crime. In the real world, proximity is frequently a necessity for a successful crime. Much traditional crime requires the physical presence of the criminal and is done face-to-face and one-on-one. Not so with cybercrime which can be done at a distance and (as anyone who has received a Nigerian fraud solicitation knows) in bulk on a one-to-many scale. And because the physical presence requirement helps to delimit physical criminality, it also makes capture easier – a factor whose absence makes identifying and prosecuting cybercrime a significant challenge.

Thus, today we face a vexing situation, where high-profit criminality can occur with low risk of capture. This turns our deterrence model of law enforcement on its head. Deterrence only works when there is a credible threat of response and punishment (the degree of punishment mattering less than the degree of certainty of being caught). But deterrence cannot work without attribution and the nature of cyberspace makes attribution viciously difficult.

Finally, there is a cultural dissonance between the public's view of traditional crime and the dynamics of cyberspace. Law enforcement professionals generally focus on solving crimes. Despite changes occasioned by the response to September 11, they continue to do less work on prevention. Likewise, the public tends to leave "prevention" to the professionals. What little prevention we do is generally defensive in nature (e.g. putting locks on doors) and leaves offensive investigative function to others. Thus the dynamic is for the public to take relatively little responsibility for its own protection – again, an understandable policy when the neighborhood police patrol can be effective, but not the best posture when the criminal "neighborhood" is global. In effect every computer is a border point – between countries or for entering a home. We have yet to fully come to grips with that reality.

International law – How does the law of armed conflict apply to a putative cyber attack?

To begin with, before considering the law of armed conflict, it is essential to define the appropriate conflict management principles for assessing whether and when a State can use force. The paradigm, of course, is that States may legitimately act in their own self-defense under Article 51 of the UN Charter when confronted with an armed attack.

The first question, then, is how one assesses whether a cyber attack, in some form, may be characterized as an armed attack? This is especially difficult, because there is no international consensus on the definition of what constitutes an armed attack, even in the kinetic sphere. Generally, however, such an assessment looks to the scope, duration, and intensity of the use of force in issue.

This ambiguity in the kinetic arena has carried over into the cyber domain; however, there are three schools of thought regarding when a cyber attack might be viewed as tantamount to an armed attack. One school looks at whether the damage caused by such an attack could previously have been achieved only by a kinetic attack. For example, using this model, a cyber attack conducted for the purpose of shutting down a power grid would be deemed an armed attack, as, prior to the development of cyber capabilities, the destruction of a power grid would typically have required using some form of kinetic force. A second school looks only at the scope and magnitude of the effects of a cyber attack on a victim-State, rather than attempting to compare these effects to any form of kinetic attack (for example, the disablement of a financial network, with real effects, but no physical harm). A third view is akin to a strict liability rule – any attack on a State's critical national infrastructure, even if unsuccessful, would be deemed an armed attack per se (and thus, would cover attempted intrusions that had no consequences). By and large, the US has adopted the middle view – focusing on the overall effects of a particular cyber attack.

But, even here, there is no consensus. There are, of course, some relatively easy cases. Data exploitation without damage is almost certainly not a use of force. By contrast, a cyber attack causing physical damage is a use of force. The hard questions lie in the grey area. If, for example, agents were introduced into a system for exploitation and attack, but not yet activated, should that be considered a use of force? Or, to identify another issue, is the "mere" destruction of data a use of force? Some in the intelligence community might even deem aggressive "phishing" (i.e., acquiring sensitive information through fraud) a use of force.

Here, we have no settled doctrine.

Even if it can be determined that a cyber attack is an armed attack, one must next resolve whether the attack can be attributed to a nation-State. In the cyber world, attribution will often require crossing several sovereign boundaries, and if responsive force is to be used, the actions taken will occur within some other State's territory. But, in the cyber realm, a State is often not directly involved in the cyber attack; the attack is the product of independent or semi-independent actors.[2] Under what rules can we attribute their actions to a State (assuming, of course, that, forensically, we can even identify these independent actors)?

The doctrine of "State responsibility" has long been an established international law concept, but it has become particularly relevant in terms of assessing responsibility for cyber attacks. Simply put, this doctrine stands for the proposition that that every State has an affirmative legal obligation to prevent its territory from being used for attacks on other States. If a State is unable or unwilling to prevent such attacks, it can (if self-help is unavailing) be held responsible for these attacks.

Again, however, the practical assessment of State responsibility is contextual in nature. One asks whether the State has effective control of the actors – that is, the capacity to direct their actions. Failing this, does it exercise overall control of the actors – that is, while not directing their actions, does the State, nevertheless, affect the overall coordination and planning of their actions. In both these situations, there is likely State responsibility.

Finally, and most frequently, however, one asks whether the State is indirectly responsible for certain acts in issue – that is, does its failure to act constitute a basis for deeming it responsible for a cyber attack, or a series of such attacks. Here, the questions become even more indefinite. One asks whether the State has effective laws on cybercrime on its books; whether it has aggressively enforced these laws; whether it cooperates with victims in the investigation of cyber incidents; and whether the State has a long history of serving as a haven for cyber

[2] After a year of research, the non-profit US Cyber Consequences Unit recently issued a report on the Georgia attacks, concluding (with appropriate caveats regarding degrees of certainty) that they were loosely coordinated with Russian officials but likely formally independent from their control. See Overview by the US-CCU of the Cyber Campaign Against Georgia in August 2008 (August 2009) (available at http://www.registan.net/wp-content/uploads/2009/08/US-CCU-Georgia-Cyber-Campaign-Overview.pdf).

attacks.

Balanced against this is the reality that some attacks (for example, by botnets) truly have no geographic source. They are transnational in nature, straddle multiple borders, and are derived from the acts of coalitions of individuals residing in multiple jurisdictions. As this discussion makes clear, application of the State responsibility doctrine to cyber attacks is likely to be both highly contextual and controversial on the international stage.

Thus, in the international law realm, as in the criminal realm, many problems arise from lack of attribution. President Obama's recent 60-day review of cyber policy recommended that strong efforts be made to solve this issue and to build better means of identity management into the system. The technology does not allow for this now, but that can change – and until it does attribution questions will remain exceptionally challenging.

This will especially be so when one adds a political overlay to any incident (as will inevitably be the case). Imagine, for example, a cyber attack on the Federal Aviation Administration and/or the New York Stock Exchange that results in significant public disruption. Even if attribution is uncertain, the public dynamic will pressure US leadership to respond. A realistic appraisal is that they will be willing to do so with significantly less than 100% certainty of attribution – with the concomitant danger of incorrectly attributing the source of the attack. The first cyber war might well start by mistake.

Only if one answers the "armed attack" and "attribution" questions satisfactorily can you then turn to determining whether a use of force response is appropriate under the law of armed conflict. That law, of course, provides that a state may use a justified, proportionate use of force. To determine proportionality, we (yet again) turn to a multi-factored analysis. Those advising on this matter will be obliged to determine whether a use of force response is militarily necessary or whether the incident at issue could be resolved in another manner? Is a planned use of force response proportional in nature? That is, is the degree of force to be used excessive, when balanced against the value of the military objective sought to be gained? Does it adequately distinguish between military objectives and civilian property?

These questions are particularly indeterminate in the cyber context. Nobody can definitively say, in every situation, what an appropriate "non-kinetic" cyber response might be. And those responses we can imagine (hacking back into

an adversary's systems, for example) might cause collateral damage to civilian property or systems that is disproportionate in nature (often because, in the cyber realm, they are inextricably intertwined).[3]

In short, for issues of this kind, no consensus exists among international law practitioners. Creating more law may not help, however, as such decisions will always involve subjective judgments based often on ambiguous facts.

What is certain, however, is that these decisions are fraught with national importance. It is likely, therefore, that they will need to be made at the highest levels of government, and not at the level of, say, a DoD systems administrator. But, even the identity of the appropriate decision-maker is uncertain. The Commander of Strategic Command has said that he believes he can make the decision to respond to a cyber attack degrading US defense capabilities. Some in the Air Force, focusing on the speed of cyber events, have suggested that there is a need to develop an automated response for certain cyber scenarios. Most of the participants in the workshop were of the view, however, that because there currently exist no definitive rules of engagement for cyber war, at least as a first approximation, all decision-making will have to be conducted at the level of the National Command Authority.

Finally, we recognized that, to be effective in this decision-making, our leaders will require sophisticated technical advice. As one participant noted (with tongue only partially in cheek), "if your cyber advisor isn't under 35, you have the wrong advisor."

Intelligence Law – For the most part the laws of intelligence collection have applicability to our cyber activities in two contexts: as rules of authorization and limitation within the domestic sphere and as rules of public disclosure. They have much less to say, however, about the nature and scope of permitted offensive collection activities overseas.

First, and foremost, intelligence law serves to delimit the nature of intelligence activity that US officials may undertake, especially when operating domestically.

[3] In 2003, the United States reportedly considered a cyber attack on Iraq's financial network to be conducted in coordination with the kinetic war that occurred. It is said that fear of uncertain collateral consequences caused the United States to refrain from the planned attack. See Markoff & Shankert, Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk, New York Times (Aug 1, 2009).

In general, the purpose of the domestic law is to permit the exploitation of foreign intelligence sources while protecting American civil liberties. It also serves as a bedrock foundational source for the authorization of all national intelligence activity.

Thus, we begin by recognizing the inherent constitutional authority of the President to respond to an attack, even if only a cyber attack, as part of his executive authority. This may well involve the deployment of intelligence (as well as military) resources. Beyond that, however, we need to understand precisely what Congress has authorized the government to do, if anything. There are few cyber-specific authorizations (with the possible exception of the Computer Fraud and Abuse Act). There are, however, a number of authorization and limitation laws of general applicability – the Neutrality Act, Foreign Intelligence Surveillance Act, Posse Commitatus, War Powers Resolution, and the foundational laws creating the intelligence operations of the United States – whose terms will bear on and limit intelligence activity.

Secondarily, legal questions will also arise concerning the disclosure of the results of the government's intelligence analysis. This will have particular saliency when we examine questions of supply chain security (or, more accurately, insecurity). The government, of course, is concerned with the intrusion of corrupting hardware and software into products that it uses. It may, for example, be concerned about chips manufactured in China. And, as with all things in the cyber domain there are varying level of certainty with which the intelligence community can draw inferences about the risk. While it may be in a position to say that the risk from a purchase is "high" it can never say it is absolute.

How then to respond to an inquiry from a domestic company that is also considering a systems purchase – especially, say, an inquiry from a company that provides support to the US defense or intelligence communities through its own manufacturing. Under current law, if such a company inquires as to the government's knowledge about a supplier, the unfortunate answer they must receive is "we can't tell you." The intelligence community has no authority to create, in effect, a black list of suspect suppliers in the supply chain.[4] And in any event,

[4] There are, to be sure, authorities under which the US government may suspend or ban a company from providing supplies under contract to the Federal government. Those authorities are, however, often cumbersome to use and may require degrees of certainty regarding risk that are not inferable from existing intelligence.

the effort would create all sorts of potential liability questions: How certain are you? How often must you update or modify your assessment (and what would be the resource commitment to do so)? In short, the intelligence community can, and does, share such concerns within the US government but is presently legally disabled from disseminating the same information to critical private-sector stakeholders. This is one legal area that clearly requires work.[5]

But all of this is, of course, about domestic law and the intelligence communities' obligations under that law to American citizens. In the context of foreign laws or international law, espionage is sometimes characterized as lawless. When exploiting sources overseas the premise is that good work is all about breaking the law of some foreign jurisdiction. Without doubt any cyber espionage done by US assets in, say, China, violates domestic Chinese law, but it is of little concern to American law.

The question is slightly more complex when one considers applicable customary international law. Here the uncertainties are greater – both as to the content of the law and as to its binding nature. While some international norms are absolute and accepted by the United States, most international legal questions have indefinite answers. When asked: "can I do this?" the answer, most frequently is "maybe." If certainty is required before action is taken, sovereign actors will be immobilized, because certainty is rarely possible. Perhaps the best a policymaker can hope for is a determination that there is both doubt and enough justification to act. At bottom, then, international law questions often involve non-legal issues – rather, they are mostly disguised political concerns about how actions will be perceived by others.

Thus, while the law of other sovereigns and international norms will have some impact on decision-making with regard to intelligence activities, the predominant determinant of lawfulness is, and is likely to remain, domestic law.

Privacy and Civil Liberties – In all of these areas (but especially in the criminal law and intelligence law contexts) most workshop participants agreed that civil liberties issues are acute. The American people not only need to know, at least in a general way, about US cyber policy, but they also must be assured that their 1st

[5] The Economic Espionage Act of 1996 is available for domestic purposes, but it has been an underutilized tool of law enforcement. See Harvey Rishikof, "Economic and Industrial Espionage," in Vaults, Mirrors & Masks, ed. Jennifer E. Simms and Burton Gerber, (Georgetown University Press, 2009.)

and 4th Amendment rights will not be compromised without a serious consideration of both the national security interests and the countervailing liberty interests at issue.

Given the novelty of the privacy and civil liberties issues involved we have yet to develop a satisfactory doctrinal approach for addressing them when they are implicated by activities in the cyber realm. Statutes of general applicability, such as FISA, the Privacy Act, and the Electronic Communications and Privacy Act (ECPA), may require modification to keep up with an ever-changing technological environment. Structurally, we have begun to consider systematically privacy and civil liberties issues through the institutionalization of privacy officers in most of the Departments with cybersecurity responsibilities. But some workshop participants thought that more needed to be done, both to enhance transparency of governmental policy and to institutionalize oversight as a protection against governmental abuse. Appointing members to the statutorily mandated (but still vacant) Privacy and Civil Liberties Oversight Board would be a good first step in this direction.

Default Rules and their Development – So, we have three distinct legal régimes, each of varying degrees of specificity and permissiveness and each with distinct procedural and doctrinal ground rules. In some cases it will be relatively easy to determine which of these legal systems applies to a particular case. But often (especially when the cyber world is at issue) sourcing and motive are ambiguous. A criminal fraud hack looks very much like an effort to take down a financial network preparatory to a war and both might easily be confused with a Chinese intelligence intrusion. When we can't tell what is happening with precision, how do we know which law to apply?

The threshold of which category to apply is critical. In general, situations of ambiguity such as this call for the development of the different régimes of law toward convergence. Until that is possible, however, we will need to develop default rules that presumptively guide behavior, until the facts on the ground counsel differently.

We already have done this through an ongoing organic process. A fair assessment is that current American doctrine has trended toward the default position of treating intrusions as law enforcement issues. But the truth is that applying the criminal law is of limited utility. As one participant noted, criminal law is so cumbersome that when it is successfully applied we are "only catching the stupid people." Sophisticated criminals (and terrorists and government intelligence

operatives) will be hard to catch using traditional criminal law methodologies.

Making the criminal law the dominant paradigm may also be tying our own investigative hands. Under the Computer Fraud Abuse Act, could an attacked entity legally "hack back" at its attacker? Could it set up honey pots to catch intruders? Probably not. Application of the CFAA (as well as the ECPA and Title III) make it doubtful that any public or private American entity can effectively exercise self-help in responding to cyber intrusions without itself violating the law.

This is not, of course, to say that criminal law is deficient. It is relatively complete and satisfactory within its own domain and, in fact, it may be the best of a limited option set. For one thing, it (along with civil law) is the most protective of American citizen's interests and offers them greater protection. When the FTC recently shut down an ISP for hosting a criminal Russian enterprise, the ISP was at least entitled to contest the action.[6] By contrast if, say, a military paradigm were the default rule, private actors would be faced with more problematic questions regarding their role in the "war." Their servers and networks would be subject to attack and they might be viewed as combatants in the war – a status that private actors are likely to wish they did not have.

Moreover, the organic method of developing doctrine through executive consideration seems to be the only one available at the moment. Given the complexity of this area of law and the practical challenge of finding political will to motivate Congress to legislate on this issue, this is unlikely to change in the near future.

Hence the only venue for change and, if possible, convergence will be through executive action. One final thought would be to consider that such doctrinal and legal development be conducted in as transparent a manner as is feasible. To the extent possible, discussions about cyberlaw, doctrine, and policy should not be classified. While in some instances the disclosure of doctrine may be impossible (lest sources and methods be disclosed), for the most part the public revelation of our response doctrine will be to our benefit. Doing so will create international norms for behavior and then, collaterally, attach a stigma to those who fail to to

[6] See FTC v. Pricewert (N.D. Cal. June 1, 2009). The FTC's complaint is available at http://www.ftc.gov/os/caselist/0923148/0906043fncmpt.pdf; see also Court Shuts Down 'rouge' ISP After FTC Complaint, PC World (June 4, 2009) (available at http://www.pcworld.com/article/166130/court_shuts_down_rogue_isp_after_ftc_complaint.html?tk=rel_news).

conform. Moreover, a robust doctrine can serve as a deterrent.[7]

One must understand that norms and stigma are rather thin reeds for the development of a global legal doctrine for responding to cyber incidents, but the diversity of views around the world makes a coherent and enforceable legal régime a distant reality. These norms would be, in the workshop participants' view, a good first step.

[7] Indeed, a standard may well develop even if the United States does not participate. As noted in Chapter 1, Canadian researchers asked to examine intrusions into the Dalai Lama's network opened a window into a broader operation that, in less than two years, has infiltrated at least 1,295 computers in 103 countries. Under present laws, it is doubtful that United States law would permit that kind of sleuthing.

Chapter 4
Form and Function- What Organization is Required?

In government, policy gets made in three distinct ways: First, it is often created by a top-down directive (e.g. to fulfill a campaign promise) and the goal is to determine the best construct to achieve the already identified objective. Second, it is created from the bottom up, reflecting a determination to ask the subject matter experts to develop their best response to a problem and propose a coherent solution. Third, it simply "happens" – a major event will force action to be taken immediately. Even in the absence of any law or policy the need for an immediate decision comes first and drives outcomes.

Government Organization – For the most part our cyber policy thus far has been a combination of all three modes of policy development, with a strong emphasis on the later, ad hoc policy development meme. President Obama's 60-day review provides us a good opportunity to step back and suggest some principles for a coherent cyber strategy.

One issue to address is determining how best to organize our government to act. But it is appropriate to defer deciding an organizational structure until we decide what the problem is and what the essential solution set is. Form should not come before function.

Broadly speaking one may assess the critical problem as protecting the President's ability to communicate with and in confidence to his subordinates and protecting their ability to act to implement his directives in a manner that is not impeded by external cyberthreats. Secondarily, we assess the challenge to be protecting the economic stability of the United States from disruption. To achieve this we believe the government needs better real-time awareness of what is happening on the networks.

This requirement (primarily defensive in nature) raises six distinct sub-issues that will affect how a government-wide response is structured:

•Any structure will need to be capable of resolving the tension between sharing information and the need for secrecy. As noted in Chapter 2, this recurring theme pervades both governmental and private sector responses;

•Any policy determining structure will need to be closely coordinated with the

Office of Management and Budget. Within the federal government, at least, governance decisions are often reflected in (and determined by) funding level determinations;

•Any structure must also take account of the structure of congressional oversight, which produces fragmented guidance and funding decisions (and which historically has been difficult to reform);

•The structure must foster investment in critical research issues of attribution and authentication and the development of secure hardware and software;

•The structure must account for and resolve complex inter-agency relationships (e.g. between NSA and DHS and between NCIX (the National Counter Intelligence Executive) and the new Cybercommand in DoD);

•The structure must also foster openness on decision-making for all Americans to participate and insure that privacy and civil liberties concerns are taken into account in designing operational solutions.

Currently, most workshop participants perceive that there is no suitable governmental structure in place to achieve these objectives. More significantly, it seems clear that the most significant requirement for any structure that we choose is leadership with the authority to control budgets and set priorities and policy. Given the complexity of the problem of cybersecurity and its cross-cutting nature, it will only be solved through the sustained application of attention and the capacity to compel adherence to a decision-making process to insure that decisions actually get made.

On balance participants recognized that the most flexible institution in the US government is the Executive Office of the President (EOP). Only the EOP has the capacity to compel everyone involved to come together and resolve issues of consequence. Without that sort of compulsory engagement, one may anticipate (at least on the government side) stasis.

One must also recognize that, especially with respect to cybersecurity issues, the US government will need to involve non-EOP and non-US government experts. External voices must be included in the discussion, however hard that is to do. Amongst the governmental actors who will need to be engaged proactively to resolve the cyber challenge, are the following:

• Chief Information Officers. The CIOs' function is to coordinate information-sharing and break down stovepipes. They are the enforcers of standards and sharing rules across domains. Security problems are integral to the CIOs' governance and management problem. And, at the core, the CIOs are responsible for the purchase of the hardware and software in which these problems appear;

• The science community, including the President's science advisor and the Office of Science and Technology Policy (OSTP) and Chief Technology Officer. They will be responsible for ensuring that research and development are directed appropriately;

• Privacy and civil liberties officers and advocates positioned to weigh in during the development of policies and capabilities;

• The Department of State, which will need to make every effort to advance our goal of international standard-setting on cybersecurity and crime issues; and[1]

• The Departments of Commerce, Treasury, and Homeland Security, each of which will need to reach out to the private sectors to build relationships.

To this list one must, of necessity, add the operational agencies with the US government that have a daily responsibility for addressing cyber threats. This will require coordinating at least four distinct streams of activity:

• Law enforcement activity, primarily conducted by the FBI, but with significant input from other federal law enforcement agencies (e.g. the Secret Service) and significant reliance on state and local law enforcement assets;

• Infrastructure protection activity, primarily conducted by DHS using its legal authorities but with significant technical assistance and input from the NSA and other intelligence community components;

• Military responses (if any) that will be directed by the DoD Cyber Command and will call upon resources from the intelligence community; and

• Intelligence activity, including both defensive and offensive counterintelligence.

[1] Russia has, for example, recently proposed development of an international treaty banning cyberwarfare. See Markoff & Kramer, U.S. and Russia Differ on Treaty for Cyberspace, New York Times (June 27, 2009). The international dimensions of the cyber domain cannot be underestimated.

Private Sector – Beyond this one sees a significant (and, indeed, predominant) need to engage private sector assets. The private sector is no monolith – it comprises security companies, router manufacturers, telecom and cell phone providers, ISPs, and more. Each addresses issues of capability and liability in differing ways. The private sector also faces significant behavioral and managerial challenges in reducing its cyber vulnerabilities – challenges that vary from company to company and sector to sector. Any organizational structure must account for this lack of homogeneity and allow consideration of many differing private sector conceptions of appropriate action.

It will also be of value to engage the private sector so that the government can pick and choose the best practices in the private sector for its own use. Some investment banks may have superior information security. Online auction systems might have good anti-hacker threat detection systems. Internet games operators have, of necessity, become highly adept at protecting their games from being compromised. The government can directly benefit from private sector innovation if the right structures are in place.

More notably, government communications (except for the very most secure) run through and on privately owned networks. Any effort to develop an intrusion detection system, for example, akin to the Einstein 3 system proposed to protect government networks, will necessarily require the cooperation of private sector telecom actors. [2] And because government communications are comingled with the private communications of non-governmental actors who use the same system, great caution will be necessary to insure that privacy and civil liberties concerns are adequately considered. Our organizational structure must permit robust oversight and early consideration of these concerns to avoid abuse.

Conversely, the organizational structure must permit the private sector to benefit from the intelligence information regarding cyber intrusions developed by the government. The government has significant capacity to identify intrusion signatures and trace attempted intrusions. This capacity needs to be suitably shared with the private sector in a manner that permits enhanced protection while protecting the government's sources and methods. This may necessitate, for

[2] The current government solution for cyber intrusions, Einstein 2, observes malicious intrusions in real time and creates alerts that are then distributed within the government. Einstein 3, which is now in development, would, conceptually, create inspection nodes on private networks that both detect malicious intrusions (as Einstein 2 currently does) and take immediate steps to prevent propagation of the malicious code. Many of the details of how Einstein 3 will operate remain classified, but the existence of the proposal has been publicly confirmed. See Nakashima, Cybersecurity Plan to Involve NSA, Telecoms, Washington Post (July 3, 2009).

example, a small highly classified shared space for the exchange of information, with strong protections and equally strong oversight.

Finally, the private sector will need to be engaged as we consider how to re-configure the existing system to improve its security consciousness. As one participant noted, the "fundamental architecture of the internet is sand." This is an aspect inherent in the network systems design from the 1970s. At that time the network was designed for a different threat model. System protocols were configured in a manner reflecting the fact that the network was unreliable and the trust anchors were the other people on the system – a relatively small universe who were known to each other. Today, the opposite holds true: the networks are trustworthy and work, but the people are not well known and cannot be relied upon.

Thus, we currently have no systematic defense to cyber vulnerabilities and are condemned to using "patches forever." Organizationally, our objective should be to foster an ability to build security into cybersystems from scratch. This may well require adopting new technology that rebuilds the system. Any governmental organization must, at a minimum, engage those who would construct such a system to determine its parameters and, if necessary, mandate certain aspects of it.

Interagency Coordination – For a number of years, cybersecurity was a "small" problem, in the sense that breaches were infrequent and the offense and defense were in relative balance. As one participant noted, 10 years ago when the US government did signals interception and intelligence, the frequency of successes would be scored something like a soccer game (1-0 or 3-2). Today if we were still using the same scoring method the score would be something like 922-786 and the United States would be losing. Our adversaries have greater imagination and fewer restrictions and they are, in effect, robbing us blind. Everything we do is likely to be known to them because we have no effective defense. Good offense (which the US continues to employ) is not a good defense.

Our challenges are therefore technological in nature. To improve our defense, we will require strong interagency coordination. The law enforcement community has an interest in the outcome but lacks the counter-cyber capabilities necessary. DHS likewise has the statutory mission to protect critical infrastructure but lacks the technical expertise. Meanwhile DoD (and particularly NSA) has significant technical capacity but lack statutory authorities. The military interest in protecting civilian infrastructure is made more acute by military dependence on that infrastructure. But its engagement will, for historical reasons, raise significant

privacy and civil liberties concerns. As a consequence our organizational architecture will need to manage these disparate capabilities in a way that fosters cooperation, rather than competition.

Likewise, the organizational structure will need to foster an improved capacity for offensive cyber operations. We may need to use covert actions against our adversaries and the difficulties of attribution that are so great a defensive problem become, in the offensive context, an opportunity. We will want to develop structures that permit lawfully authorized covert cyber intrusions without risk of public disclosure of specific operations or methods.

Leadership – But whatever organizational structure we choose in the end, the fundamental question will come down to one of leadership. Thus, while most workshop participants endorsed the need for a White House coordinator to engage the private sector and ease the interagency confusion, the mere appointment of a coordinator will not solve the coordination problems unless the appropriate authorities are given to the office. Those problems may only be resolved by sustained, consistent high-level attention.

In short, no organizational structure will work if cybersecurity is not made a sufficiently high priority. Today, the public remains comparatively disengaged from the cyber vulnerabilities at hand. As one participant noted, a recent theft of $16 million in a cyber fraud didn't make any major newspaper – one of the editors had asked "did anyone die?" and when told "no," spiked the story.

It would be in the nation's best interest if the government and the private sector could find the resources and attention to focus on this problem without the necessity of a crisis response driven by a digital Pearl Harbor. But in the absence of leadership and public engagement, we fear the lack of political and economic will to address the pressing vulnerabilities we see.

Thus, a critical role that organization will play is as a signaling device. If the organizational structure we choose – a strong Cyber Czar, for example – signifies high level attention and the ability to make decisions and get things done, we will have the right answer. If the organizational structure signifies a diminished level of interest, then that will, effectively, doom the substance underlying any initiative. Today, the opportunity exists for significant improvement through concerted effort – it would be a shame if that faltered for lack of high-level engagement.

Chapter 5
What Will the Future Bring?

We have examined some of the legal and organizational issues that face us. We have identified some of the threats and the American response thus far. Now we turn to our crystal balls. What will the future bring? What do we think is necessary?

New Technology – We believe there is no silver bullet technological solution to the cyber threat. Given the pace of technological development, defensive measures will always trail offensive ones, at least for the foreseeable future.

That having been said, we assess that there are feasible technology advances whose development will enhance cybersecurity. Currently, our cyber defenses are mostly limited to efforts at intrusion detection and communications monitoring. These are useful, of course, but (as we have already noted) in the absence of strong authentication and attribution systems they are of limited utility, serving principally defensive purposes. Thus we will want to foster stronger efforts at authentication for the positive purpose of authorizing access to systems, as well as for the attribution of negative efforts. To support intrusion detection we want, as noted above, to build structures that foster information-sharing in secure ways.

But these systems-based technologies will not be adequate by themselves. So long as computers execute code and insiders have access to computers there will be vulnerabilities. We foresee greater emphasis on systems that monitor network behavior. Already systems (akin to those used by credit card companies to detect fraud) are capable of noting unusual system activity (e.g. messages sent at 3 AM; large packet volumes or anomalous use signatures). These and other intrusion detection systems will need further development.

The greatest current problem, however, is and is likely to remain human factors. Passwords are chronically weak, reflecting their origin as an accounting mechanism rather than as a security feature. These weaknesses also reflect the continued resistance by users to strong password and encryption requirements. No doubt this reflects an instinctive resistance based upon natural key management challenges – people simply cannot or will not use strong passwords that are hard to remember. Nonetheless, it remains a matter of some urgency that we maintain a continued focus on training and education of users as a first line of cyber defense.

We also foresee several more systematic developments that are likely to change

fundamentally the nature of cyberspace and thus the cyberthreat: the growth of cloud computing and the re-engineering of information systems.

Cloud Computing[3] – Increasingly, multiple systems are running in a cloud environment and those systems may run on multiple machines. Under many circumstances this will mean that it is more difficult to construct malware that has machine level effects. When malware attempts to execute in the cloud context, it does so on software that emulates a hardware device, rather than on the hardware itself. This often limits or modifies the malware's capacity for harm.

Systems are moving in this direction because it is far cheaper to maintain data and applications in the cloud. For many applications, it also appears to be fundamentally more secure and resilient than local machine based operating systems.

What this means is that cyber attacks may be significantly harder to accomplish in a cloud-oriented system. By its nature the cloud permits the creation of systems with different trust levels at different tiers of interaction. At the client level where most individuals and applications operate there can be an integrity check to ensure legitimated access but one may provide only limited logical capability. Hence the capacity for malfeasance is potentially limited by the structure of the system. To put it colloquially, a gamer in Worlds of Warcraft is inherently incapable of corrupting the game.

But this also creates greater potential for catastrophic vulnerabilities that will need to be guarded against. Security works at the client level in cloud systems precisely because the cloud system owner is, in effect, "god." Thus, a successful attack at the next higher, "god," level will have even worse consequences – one may not even know if the system has been compromised. Of equal concern is the challenge of identifying a trustworthy "god." Cloud computing may make human factors issues less frequent, but the effects of a security compromise may be much greater. Who would we trust to be the "electrical grid god?"

Another consequence of the trend toward cloud computing is that the cloud makes anonymity much easier to achieve. This is so not because anonymization

[3] Cloud computing is a style of computing in which resources (that is, infrastructure or software) are provided to a user as a service through the Internet. A local user requires only an internet connection and browser software to use cloud resources. An example of cloud computing is the Google program GoogleDocs, which stores a user's written product in the "cloud" of the internet, rather than on a local hard drive.

techniques are better in the cloud. Rather, it is because information is not held in a single discrete location. One may readily foresee significant challenges in adapting place-specific concepts of American constitutional protections in the Fourth Amendment to a context where the "place" to be searched and the "thing" to be seized simply don't exist in any identifiable form. Indeed, in response to this conundrum the government may decide to mandate some form of guaranteed responsiveness. If cloud owners can't pull the information necessary for government intervention, governments around the globe may adopt CALEA-like mandates for the cloud. [4] In any event, the trend towards cloud computing will exacerbate the problem of attribution, not ameliorate it.

Information Management – Another likely future trend will be better, re-engineered information management systems and requirements. Because secrets will become increasingly harder to protect and information will be more ubiquitous, one can anticipate an effort by actors to limit or eliminate the necessity of maintaining secrecy in the first instance.

Most private sector actors are just beginning to apply this new structure and modify their behavior accordingly. Currently, many protect all the information that they have equally. But increasingly they are coming to recognize that this is both unnecessary and costly. A restructuring of their information management systems should, broadly speaking, recognize three different categories of information:

• Information currently collected but which need not be. For example, retailers will come to recognize that they often do not need to collect the financial information of their clients. A token of some form that authenticates identity will be more than adequate to insure payment. If financial information is not collected in the first instance, protecting it becomes unnecessary.

• Information necessary to run the entity's operation but which has no external use. This category would include, for example, marketing information or stock ordering and pricing data. Here, the data is of limited use outside the entity, hence it is an unlikely target for theft, except perhaps by a competitor. The principal questions will be issues of backup and resiliency to maintain continuity,

[4] The Communications Assistance for Law Enforcement Act (CALEA), Pub. L. No. 103-414 (1994) (codified at 47 U.S.C. §§ 1001-10) enhances the ability of law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment to ensure that they have built-in surveillance capabilities. Utilizing these capabilities federal agencies may, when authorized by law, monitor all telephone, broadband internet, and VoIP traffic in real-time.

with security issues secondary.

• The "crown jewels." Intellectual property and other proprietary information whose disclosure would damage the institution. Properly identified, this volume of data is much smaller and therefore protection is much more manageable.

International Cooperation – Because the clouds are not national entities, one can anticipate that their growth will put even greater emphasis on the need for international cooperation to counteract malefide actors. That must mean that subpoenas and other requests for assistance have to be effective internationally.

Realistically, one cannot anticipate uniform cooperation around the globe. The Council of Europe model has provided for consistency of process across some jurisdictions. But it is of limited utility. The process permits assistance to preserve data and allow for attribution, but it is very slow. Our experience is that it is not effective in context of the microsecond computer-hopping intrusions. The scale and complexity give these criminal investigations a very low prospect of solving the problem. More significantly, the "problem" itself changes every 3-4 years. We are struggling to get nations to adopt and implement the Council of Europe approach, but given the growth in cloud computing it may be an out-of-date solution before the ink on its signature line is dry.

We do, however, see some hope in combating cybercrime in the international environment through engagement. More can be done through the UN to devise cyber norms and rules. Diplomatic initiatives like the OECD's Financial Action Task Force have used international standards and shaming to cause countries to improve their responses to money-laundering issues. [5] A similar effort (call it a Cybersecurity Action Task Force, if you will) might yield some results in the cyber domain.

The challenge, however, will be that efforts to combat cybercrime may also be seen as efforts to restrict and limit cyber espionage and other nation-state cyber activities. Despite having common ground in fighting criminality (generally) we cannot be sanguine on the prospects for an international agreement delimiting all forms of cyber warfare; the advantages of having a cyber warfare capacity are simply too great for many international actors to abjure its benefits.

---

[5] The Organization for Economic Co-operation and Development (OECD) has chartered the Financial Action Task Force (FATF) to combat money-laundering and terrorist financing. Currently, 34 member states cooperate through the FATF to set standards, monitor compliance with those standards, and identify new and ongoing financial threats. See FATF Revised Mandate 2008-2012 (available at http://www.fatf-gafi.org/dataoecd/3/32/40433653.pdf).

Gated Communities – Given the challenges to security in a cloud computing world and the dim prospects for effective international cooperation, many workshop participants gloomily anticipate a further degradation in international cybersecurity. Some portions of the system will take on an almost "Wild West" character. To combat this, some anticipate the development of segmented gated communities on the system. Entrance to these systems will be carefully monitored and available only to trusted participants who agree to give up their anonymity to some degree and allow strong attribution of their actions.

These trusted communities will not, of course, be pervasive. And they will only be successful to the extent that strong intrusion detection and behavior monitoring technologies are developed. But given the vulnerabilities that exist in the unregulated cyber domain, one can fully anticipate that many users will, in the long run, gravitate to a more secure, albeit more isolated, domain.

This trend will mean, naturally, that users will move away from the current vision of a singular internet and net neutrality. But such trusted networks already exist (e.g. SIPRNET or JWICS in the US government). [6] One possible future will likely see the recreation of walled gardens like those that were developed when AOL was first exploring internet access.

More Speculation – Overall it is likely that cyber technology will continue to develop at a faster pace than cyber policy. Absent corrective action this will continue to magnify the tragedy of the commons afflicting cyberspace. The gap between policy and reality is widening not narrowing and we cannot manage our way out of the problem.

In the face of that tragedy and in the absence of effective governmental action we may see self-help networks develop within the private sector. The private sector is already developing analytical tools to use in identifying the source of intrusions. One may expect it to develop other self-protective mechanisms like reliable supplier lists. Government may make its best contribution to cybersecurity by authorizing private sector action and then getting out of the way.

This empowering of the private sector would complement a revision to our cur-

[6] SIPRENET and JWICS are classified US government systems handling, respectively, Secret and Top Secret level material. They are interconnected between government users but physically isolated from unclassified computers.

rent approach to cybersecurity, which is best characterized as the "professionalization" of security – protection is left up to the professionals who "know what they are doing." A different approach would adopt an open security model and try to make cyberspace safer by making cyber activity more visible to everyone. This is, in effect, a completely different security model utilizing a fully open environment. If everybody could, for example, see what the Chinese were doing now, they might have another reaction. The growth of Web 2.0 systems permits responses of social shunning and transparent exposure instead of relying on proprietary security responses. Security then starts to look more like a public health model, in which the system brings all available resources to bear against a problem.

Notwithstanding the potential for private sector self-help, government may also need to "semi-nationalize" some sectors (like the electricity grid) where isolation is not an option and the adverse consequences of certain low probability events are likely to be very high. For these critical infrastructure systems semi-nationalization would provide access to intelligence assistance and liability protection, in exchange for an even greater loss of independence.[7]

Finally, to reemphasize a point made earlier, the future looks dim in the absence of leadership. Other countries are looking to America and American ingenuity to solve the cyber problem. The question is: Do we have the national will to make this happen? One hopes so, for we are quite certain that a worse situation will result if a leadership vacuum caused by America's failure to engage is filled by China or Russia. America is still seen as an international leader and the US needs to be responsible for the development of a global cyber solution. We're at a critical juncture, and if the US does not act, someone else will fill the space.

[7] Many of these sectors are natural monopolies that are already highly regulated.

Chapter 6
Metrics for Success

The system today is in a crisis. That crisis is one that is only slowly becoming clear and achieving public awareness – but we stand at a crossroads.

Today, determined adversaries can enter some classified systems undetected, encrypt data while in the systems, extract it, and leave behind autonomic tools that will dial back to the installer, over time, at a time of his or her programmatic choosing. That is an immensely serious concern. And if that can occur on classified systems, imagine what is happening in the unclassified domain.

Most kinetic threats we will face can be thought about well in advance and can be prepared for. The cyberthreat will be executed in millisecond time with enduring consequences. If the Chinese military were at our borders ready to attack we would deem that a crisis. Today, in the cyber domain, we are effectively at the same place. Questions remain:
• How will we know when the crisis is over?
• How will we know if what we are doing is effective?
• How do we know if we've won?
• Or, put another way, given President Obama's commitment to the creation of a new "Cyber Czar" position within the White House, how will we know if the czar has succeeded?

In asking these questions, we want to move away from traditional Washington metrics of success. By these standards, the czar will succeed if the staff and budget increase exponentially. The czar will be a real bureaucratic success if a fight with some in-house adversary is won. And the czar will be a failure if some cyber-Pearl Harbor occurs on his watch and the czar is forced to resign.

None of these are, of course, real measures of success. They assume a myopic "inside the Beltway" vision of reality in which only your press releases count. Real success will be difficult to measure. We cannot, for example, say whether a reduction in the number of intrusions detected reflects our success in preventing them or a growing capacity on the part of the intruders to evade detection. Indeed, our only true measures of success are likely to be indirect ones that serve as proxies for our ultimate goal. But if we were to suggest some realistic measures by which our success over the next 4-8 years could be measured, the following would be a non-comprehensive list of metrics that ought to be considered:

Have we reduced the number of intrusions into American governmental systems?
- What degree of success do NSA red teams have in penetrating our networks?
- Are we more effective at the attribution of malefide actors?
- Have we improved encryption standards?
- Does intrusion detection lead seamlessly to immunization and prevention, such that intrusions by a particular method are a one-time-only occurrence?
- Have we adopted an effective identity management system (more or less premised on the one outlined in Homeland Security Presidential Directive-12)?
- Is America more successful in offensive cyber intrusions than its opponents are (i.e. are our offense and defense better than that of our opponents)?
- Have we enhanced coordination and agility in responding to events in a way that makes a Cyber Czar no longer necessary?

Has the private sector adopted appropriate security measures?
- Have we increased the application of patches for vulnerabilities that are known to exist, where lethargy has delayed or prevented application?
- Are auditing schemes generally in place? Have they resulted in the adoption of generally accepted best practices that embody standards of care that the courts deem significant?
- Is private sector R&D increasing?
- Is there an appropriate liability régime in place that allows injured parties to seek compensation for consequential damage?
- Have we found ways to incentivize resiliency?
- Are we devising a more secure system architecture for the cyber domain? What are the prospects for its adoption and implementation?

Have we developed a doctrine of cyber warfare and response?
- Do we know how we will respond to an overt cyber attack that causes physical damage?
- Do we know what our response will be to a covert intrusion?
- Have we defined what constitutes an armed attack and when we will attribute that attack to a State actor?
- Has the law of armed conflict reached consensus on the definitions of lawful and unlawful use?

Have we improved international cooperation against cybercrime?
- Are international requests for assistance routine and effective?
- Is information shared internationally quickly enough to have effect?
- Are the numbers of safe havens for cybercriminals being reduced?
- Is there international agreement on norms of behavior that have the effect of modifying the behavior of state actors?

Have we internalized within the US government conceptions of cybersecurity that are currently lacking?

- Does procurement policy take account of cyber vulnerabilities?
- Are there new federal acquisition rules that incorporate cybersecurity standards for all hardware?
- Does OMB fund cybersecurity projects adequately?

Have we taken leadership of the cyber issue?

- Is there a national strategy in place that identifies roles and responsibilities throughout government and in the private sector? Is it a paper strategy or is it actually being implemented?
- Does the American public understand the scope and nature of the cyber problem?
- Do they care about it and have they considered how cyber issues impact privacy and civil liberties?
- Have we changed the public's mindset of cybersecurity so that good practices are well accepted (much like wearing a seatbelt is now considered the norm)?
- Is more attention being paid to cyber conflict in the academy?
- Has transparency increased, thereby enhancing public debate on the appropriate solution set?
- And the single key metric, which is almost immeasurable:

HAVE WE EXERCISED VISIONARY AND COURAGEOUS POLITICAL LEADERSHIP TO FORMULATE A COHERENT POLICY?

*****

Every era has its enduring images. We are now more than 60 years from the end of World War II, but the images of those events still stand in American memory – images of sunken ships in Pearl Harbor; soldiers rushing ashore in Normandy; the mushroom cloud over Hiroshima; and the gaunt faces of the Holocaust survivors.

What will be the enduring image of this cyber era? Will it be one of a darkened city, whose electric grid has failed? Will it be a picture from Second Life or the image of a computing cloud? Or will it be a picture of cybercriminals led off to jail for their attempted offenses, having been caught in the act? Only time will tell. We are, however, convinced that we stand at the crossroads – the decisions we make today will help determine the defining images of tomorrow.

Appendix I: list of Workshop Participants

The Honorable Joel Bagnal
President
Detica, Inc.

Stewart A. Baker
Partner, Steptoe & Johnson LLP

Brad Barker
President
The HALO Corporation

Marjory S. Blumenthal
Associate Provost, Academic
Georgetown University

Spike Bowman
Distinguished Fellow
University of Virginia School of Law

Joel F. Brenner
National Counterintelligence Executive
Office of the National Counterintelligence Executive
Office of the Director of
National Intelligence

Susan W. Brenner
NCR Distinguished Professor of Law and Technology
University of Dayton School of Law

James X. Dempsey
Vice President for Public Policy
Center for Democracy and Technology

Stephen Dycus
Professor
Vermont Law School

John M. Gilligan
President
Gilligan Group, Inc.

David E. Graham
Executive Director
The Judge Advocate General's Legal Center and School, U.S. Army

Eric A. Greenwald
Chief Counsel
Permanent Select Committee on Intelligence
U.S. House of Representatives

Jessica Herrera-Flanigan
Partner
Monument Policy Group

James Andrew Lewis
Director and Senior Fellow
Technology and Public Policy Program
Center for Strategic and International Studies (CSIS)

Herbert Lin
Chief Scientist
Computer Science and Telecommunications Board
National Research Council/National Academy of Sciences

Kate Martin
Executive Director
Center for National Security Studies
The Georgetown University

Jacob Olcott
Director and Counsel
Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology
Committee on Homeland Security
U.S. House of Representatives

Scott O'Neal
Deputy Assistant Director
Cyber Division
Federal Bureau of Investigation (FBI)

S. Eugene Poteat
President
Association of Former Intelligence Officers (AFIO)

Leonard G. Raymond
Managing Member
Volvox Associates, LLC

Harvey Rishikof
Former Chair, Department of National Security Strategy
Professor of Law and National Security Studies
National War College

Paul Rosenweig
Principal
Red Branch Consulting PLLC

Marcus H. Sachs, P.E.
Executive Director, National Security Policy
Verizon

Suzanne E. Spaulding
Principal, Bingham Consulting Group
Bingham McCutchen LLP

Kim Taipale
Founder and Executive Director
Center for Advanced Studies in Science and Technology Policy

Mark D. Young
Special Counsel for Defense Intelligence
Permanent Select Committee on Intelligence
U.S. House of Representatives

Lee M. Zeichner
President
ZRA, LLC

OBSERVERS

David Anderson
Vice President of Civic Programs
McCormick Foundation

Lauren Bean
Managing Editor, National Strategy Forum Review
National Strategy Forum

Susan S. Gibson
Senior Managing Attorney
Office of General Counsel
Office of the Director of National Intelligence

Timothy J. Gibson, Ph.D.
Program Manager
Defense Advanced Research Projects Agency

Holly McMahon
Director
Standing Committee on Law and National Security
American Bar Association

Lillian Murphy
Program Manager
National Strategy Forum

Appendix II: Recommended Readings

Articles – News (Print), Online, and Blogs

•Basu, Subhajit and Richard Jones. "Regulating Cyberstalking" Journal of Information, Law and Technology. November 1, 2007.

•"Cyberwarfare: U.S. Policies Called Uncertain, Unsound" The Washington Post Nation Digest. April 30, 2009.

•Kirk, Jeremy. "Deep computer-spying network touched 103 countries" IDG News Service. March 30, 2009

•Miller, Jason. "White House cyber review is just the beginning" Federal News Radio. May 4, 2009

•Strom, Chris. "Report: U.S. Needs Policy For Attacking Foreign Networks" Congress Daily. April 29, 2009

•Sullivan, Bob. "Tech: What Will Go Wrong in 2009" The Red Tape Chronicles, MSN (Blog). December 30, 2008.

•Tennant, Don. "The fog of (cyber) war" Computerworld. April 27, 2009.

•Zetter, Kim. "Outgoing DHS Cyber Chief Expands on Why He Resigned" Wired. March 9, 2009.

•Melissa Hathaway's blog entry, with links to the Cyber Review and the individual papers that informed the recommendations, can be found at http://www.whitehouse.gov/CyberReview/
The fact sheet: http://www.whitehouse.gov/the_press_office/Cybersecurity-event-fact-sheet-and-expected-attendees/
The President's remarks are at:
http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

Reports

•Securing Cyberspace in the 44th Presidency. The Center for Strategic and International Studies. December 8, 2008. (64 Pgs.)
•Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities. National Research Council of the National Academies; Committee on Offensive Information Warfare, Computer Science and Telecommunications Board, and Division on Engineering and Physical Sciences. 2009.
•Tracking GhostNet: Investigating a Cyber Espionage Network. Information Warfare Monitor. March 29, 2009. (53 Pgs.)
•Quadrennial Roles and Missions Review Report. Department of Defense. January, 2009. (48 Pgs.)

National Security Threats in Cyberspace

♦

A Post-Workshop Report

American Bar Association Standing Committee on Law and National Security

National Strategy Forum

Underwritten by McCormick Foundation

September 2009

Printed Courtesy of the HALO Corporation
WWW.THEHALOCORP.COM