

CYBER DETERRENCE SYMPOSIUM

Proceedings Report

Homeland Security Policy Institute
Policy & Research Forum Special Event

November 2009

HSPI STAFF

FRANK J. CILLUFFO
Director

DANIEL J. KANIEWSKI
Deputy Director

SHARON L. CARDASH
Associate Director

JOSEPH R. CLARK
Policy Analyst

F. JORDAN EVERT
Presidential Administrative Fellow

OUR MISSION

Founded in 2003, The George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan “think and do” tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation.

HSPI would like to acknowledge the support of the Intelligence & National Security Alliance, BAE Systems, CSC, General Dynamics, ManTech International Corporation, Northrop Grumman, and QinetiQ.

OPENING REMARKS

INTRODUCED BY:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute
Ellen McCarthy; President, Intelligence and National Security Alliance (INSA)

BIOGRAPHY:

The Honorable Charles Allen; HSPI Steering Committee Member, INSA Intelligence Advisor, and Principal, The Chertoff Group

Charles Allen served as a member of the US intelligence community for five decades. Joining the CIA after graduating from the University of North Carolina at Chapel Hill in 1958, Allen retired from federal service in 2009 as the Chief Intelligence Officer for the Department of Homeland Security’s Office of Intelligence and Analysis.

The Cyber Threat Today

Allen began his remarks with a discussion of the current cyber threat. He emphasized that most Americans do not realize the magnitude of the issue, even as the threat worsens. Everyone has been touched in one way or another by these intrusions, but most fail to take actions to protect their information and data. He argued it is therefore crucial to understand the threat and frame the issues in order to mitigate negative effects.

Government Action

Allen also discussed the current administration’s efforts to safeguard critical cyber infrastructure. He noted that cyber should not be a partisan issue and stressed the importance of the National Cybersecurity and Communications Integration Center, announced by Homeland Security Secretary Janet Napolitano. NCCIC will serve as a 24-hour, DHS-led, coordinated watch and warning center that will house two operational organizations—the US Computer Emergency Readiness Team, which leads a public-private partnership to protect and defend the nation’s information technology and cyber infrastructure; and the National Coordinating Center for Telecommunications, which is the operating arm of the National Communications System. Allen stated that moving forward with these governmental projects is vital for US security because of the intrinsic value of cyberspace to modern society.

KEYNOTE ADDRESS

INTRODUCED BY:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute

BIOGRAPHY:

Jaak Aaviksoo; Estonia's Minister of Defence

Jaak Aaviksoo assumed office on April 5, 2007. His primary goals as Defense Minister were restructuring the power management of the Estonian Defense Forces and dealing with the situation of the Bronze Soldier of Tallinn, a Soviet-era war monument that was the source of much controversy and ethnic tension between a large proportion of Estonians and local Russians. Within weeks of Jaak Aaviksoo taking office, Russia launched multiple cyber attacks on Estonia.

Far-Reaching Impact

Aaviksoo began by thanking the United States for its efforts in promoting the ideals of freedom around the world and aiding in Estonia's independence. However, he warned that despite progress, the world is not much safer today. Aaviksoo believes that cyberspace is intrinsic to everything in society and that threats to the cyber realm are essentially threats to everything society values. Cyber has a far-reaching impact – from traffic lights, to airport controls, to instant global communication. These achievements are largely viewed in a positive light, but Aaviksoo pointed out that some actors use the benefits of cyberspace to do harm.

Importance of Cyber Security: Present & Future

Aaviksoo discussed the importance of cyber's impact on Estonia and the world. He noted that often one thinks of cyber as having moved into a society when in reality it is the opposite—much of society has made its way into cyberspace. The importance of cyber is illustrated in the United States by institutions like the US Air Force cyber command, corporations like RAND who regard cyber as its own medium with its own rules, and governmental agencies who rank cybersecurity high on their list of security goals. Aaviksoo observed that even national decisionmaking in Estonia has moved into the ever-evolving cyber realm through e-voting.

Strategic Communications

Aaviksoo emphasized the importance of strategic communications. He identified inadequate communication within and among member countries as one of the shortcomings of NATO. He argued that member countries' strategic communications fail to be clear, concise and responsive, and come up short in terms of credibility and effectiveness. This results in a failure to deliver consistent messages. NATO's enemies do a better job than its member countries, but by working to harness the power of cyberspace to advance communications and awareness efforts, Aaviksoo hoped this could change.

Dealing with Cyber Attacks

Aaviksoo mentioned several key issues in connection with the current approach to dealing with cyber attacks. He stressed the importance of understanding cyber attacks, which involve a constantly changing threat picture. Cyber attacks are not enabled by force, but rather by exploitation of the target's vulnerabilities. Thus, lasting defenses are impossible to build because even if the United States would be capable of defending a cyber attack today, the tools used to do so may not be effective tomorrow.

Regarding attribution, Aaviksoo argued that it is important for countries to develop understandings of responsibility for those who allow non-state actors or "freelancers" to use their territories to launch cyber attacks. On deterrence, Aaviksoo stated that a successful approach requires working with formal and informal cyber networks, and must involve the private and public sectors.

Estonian Cyber Defense League & Civilian Response

Aaviksoo noted some of Estonia's achievements in the cyber realm. The recently established Estonian Cyber Defense League allows actors to participate based on their capabilities. He asserted that because the vast majority of cyber elements are in the private sector, individual citizens are called upon in the event of a cyber attack.

Aaviksoo acknowledged that it is necessary for the government to take the lead in protecting critical infrastructure and communications. Nevertheless, he stated that the first response to cyber threats should be a civilian response, despite the fact that attacks have already occurred between nation-states.

SESSION ONE – THE CYBER THREAT

What does the cyber security threat environment look like? What challenges and opportunities exist? What leadership role should the federal government play? What posture should the United States assume?

MODERATOR:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute

KEYNOTE:

Jim Lewis; Director and Senior Fellow, Technology and Public Policy Program, Center for Strategic and International Studies

PANELISTS:

Roger Cressey; President, Good Harbor

Mike Delaney; Majority Staff Director, Permanent Select Committee on Intelligence, US House of Representatives

Sam Visner; Vice President, Strategy and Business Development for Enforcement, Security, and Intelligence Division, CSC

Overview & Background

The keynote address and panel discussion highlighted the need for conceptual clarity. Of particular concern, definitional questions about what actions constitute a cyber attack. The need for an articulated set of national interests was also identified – as was the need for consideration of the range and legitimacy of potential American responses to attack.

At the outset, Jim Lewis argued that the development and operationalization of cyber policy has been retarded by a weak methodology. To strengthen such, Lewis suggested evidentiary questions be resolved by focusing on the frequency of cyber events, their nature, and the cyber doctrine of key actors.

Throughout the discussion, the panel noted that cyber policies will be crafted and vetted for potential and realized effects on civil rights and civil liberties. The panel also noted that given the scope of cyber, any policy decisions will trigger questions regarding governmental oversight and relations between the public and private sectors.

Advantage Lies with the Attacker

Each member of the panel drew attention to the asymmetric nature of the internet's development and the resulting cyber dependency of Western populations. The panel concluded that cyber saturation, into the daily lives of most Americans and across the scope of our society's activities, heightens our relative vulnerability to attack. Thus, Roger Cressey noted, discussions of the cyber threat must originate from the premise that we will always be operating from a defensive position.

Cyber Risks

In his keynote, Jim Lewis identified three classes of cyber risks:

- espionage, a daily occurrence which includes economic activities, and is not restricted to actions taken by nation-states;
- crime, also a daily occurrence – one with the potential to provide criminals with a six or seven figure income; and,
- potential for attack, the Department of Homeland Security's March 2007 *Aurora Generator Test* proved the ability to remotely damage critical infrastructure – attackers also have the potential to disrupt data.

Cyber Opponents

Three classes of cyber opponents were also identified by Jim Lewis:

- foreign governments, the most active entities in cyber space, they have the resources, expertise, and knowledge to do the most harm – Russia and China most active;
- cyber criminals, highly skilled individuals who develop tools and techniques (such as bot-nets) to be rented or sold, often operate under implicit rules prohibiting attacks against host country – may be employed as an irregular or mercenary force by nation-states;
- political groups, primarily use the internet as a messaging tool, but have the potential to develop it as an avenue of attack.

Defining Our Nation's Cyber Interests

Sam Visner argued that there exists an underappreciated connection between cyber threats, solutions, and policy – the definition and articulation of our cyber interests. To properly understand the threat, he posited that we must understand what it is we seek to protect.

Visner charged that the first priority of any White House cyber coordinator must be to illuminate American interests and bring them in as the foundation of any cyber discussion.

For Visner, key to any discussion of interests should be the following. The US cannot afford damage to; the command and control capabilities of the American military, the nation's critical infrastructure, or its competitive advantage.

The Need for Cyber Doctrine

The need for a cyber doctrine was implicitly or explicitly expressed by each of the panelists.

Jim Lewis noted that American cyber defenses are disjointed – and lack a clear understanding of who is in charge or what role the private sector ought to play.

Roger Cressey commented that the doctrine issue is key in moving from a reactive to proactive posture.

Sam Visner stressed the need for clarity in our responses to potential attack – he offered up US doctrine concerning nuclear attack during the Cold War as a model.

The panelists made clear that American cyber doctrine would need to provide guidance concerning what constitutes an attack. For example, it would have to delineate the threshold between an act of espionage and an act of war. Doctrine would also, according to the panel, have to provide lines of and rules for communication. Doctrine would also need to supply instructions concerning the roles and responsibilities of public and private actors. So that it would provide a deterrent effect, the panelists noted that doctrine would also need to provide information about likely responses to cyber attacks.

The Path Toward Doctrine

Several of the panelists noted the importance of leadership. Lewis argued that we need to get away from the 'wild west' concept of the internet and press for better governance.

Mike Delaney noted that given the centrality of cyber to all issues of modern life, and the potential effect on civil rights and civil liberties of any cyber legislation, every member of Congress thinks they need to play a vital role in legislative debates. Delaney noted such is a real hindrance. Delaney also raised questions about just how far the legislative process ought to go and highlighted the importance of bringing in the private sector.

Cressey lamented the lack of public attention. He stated that every day we are victims of targeted cyber attacks doing real damage; yet, the issue fails to resonate with the public.

As a body, the panel argued that although cyber policy and cyber deterrence require private and public sector partnerships – what is most needed is greater presidential leadership.

Posture & Deterrence

Cressey argued that we must prioritize our critical infrastructure and that we must think in terms of resiliency. This means two things. First, we must think in terms of a cyber-Katrina, not cyber-Pearl Harbor. Second, the big issue is "how do I build trusted networks from untrusted components?"

Both Cressey and Lewis argued that the US needs to spend more time thinking about international dimensions – and the development of international norms.

Regarding deterrence, Visner argued that we must approach it as a process – not a product. Furthermore, he argued that we must be able to place something of our adversary's at risk and we need not respond in kind. Ultimately, Visner argued, our cyber strategies need to be fed into our larger global engagement strategies.

SESSION TWO – DETERRENT CAPABILITY

What is meant by “deterrence”? How would it work? Should the U.S. develop such capability; if so, why? What would a deterrent capability look like? How does attribution relate to deterrence?

MODERATOR:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute

KEYNOTE:

Michael Nacht; Assistant Secretary of Defense for Global Strategic Affairs, Department of Defense

PANELISTS:

Martin Libicki; Senior policy Analyst, RAND Corporation

Richard O’Neill; President, The Highlands Forum

Terry Pudas; Senior Research Fellow, Center for Technology and National Security Policy

Lee Zeichner; Zeichner Risk Analytics

Overview & Background

The keynote address and panel discussion revealed a consensus that passive defense, “building a fence,” would prove insufficient to protect against threats in the cyber domain. Nevertheless, the discussion featured a variety of views on what deterrence would entail and the difficulty of developing a capability.

Also up for discussion were topics including the role of the private sector, public awareness of both the threat and potential responses, and the establishment of a cyber command, co-located with the National Security Agency at Fort Meade, that will plan, organize, and implement defense of the .mil domain of cyberspace (but not .com or .gov).

Conceptual Framework

Michael Nacht categorized the threats, and thus potential targets of deterrence, as follows:

- Nation-states
 - Peer-competitors
 - Others
- Sub-national actors
 - Terrorists
 - Criminal organizations
 - Patriotic hackers
- Combinations of the above

Deterrence is difficult in a complex environment packed with a mixture of threats. Several speakers noted that because cyber attacks do not occur in isolation from other events, deterrence must fit into a larger strategic calculus that accounts for the diverse interests and motives of each actor.

Richard O’Neill urged looking at the nature of the relationships between actors and promoted a framework of “cooperation, competition, and conflict,” as “non-linear and non-discrete” categories. For example, two or more actors could be cooperating on one issue while competing on a second and in open conflict on a third. O’Neill also cautioned that thinking about conflict and methods of deterrence needed to extend beyond the kinetic perspective (see below).

Terry Pudas expressed skepticism about whether Americans had grasped the real nature of the problem and its implications in terms of operational risk and market competitiveness. Lee Zeichner argued that naming and defining is necessary to ensure that everyone is communicating with the same language and background.

Concepts of Deterrence

The panel members put forward a number of methods of deterrence:

- Threaten a potential adversary or associate with an in-kind response
- Threaten via kinetic or non-kinetic means outside the cyber realm
- Strengthen defense to the point that the adversary does not gain from attacking
- Advertise knowledge of the adversary’s actions
- Demonstrate resiliency to attack
- Create and articulate doctrine regarding cyber attack and responses
- Develop international norms and legal agreements

Attribution as a Key Ingredient

Though not the only problem, the panel members discussed attribution as the main challenge to deterrence. Nacht stressed that attributing attacks to specific actors is difficult and that the US must exercise caution, even if other states reach a conclusion.

Nacht referenced the U.S. Cyber Consequence Unit’s report on the attacks on Georgia, which concluded

that the attacks were carried out by civilians with little to no direct involvement of the Russian government or military, yet organizers had advance notice of Russian operations and objectives. They were also aided by organized criminals. This example illustrates that even when attribution is possible, challenges remain in terms of responding.

Martin Libicki addressed attribution from a definitional perspective. From a legal point of view, he said attribution asks, “Who did it?” From a policy point of view, however, the question is “Who can stop it?” In other words, the policy question centers around how the U.S. can persuade a state to prevent a sub-national actor within its borders from committing a cyber attack.

Attribution also has other problems. The more a state attributes—and reveals those attributions—the less effective attribution can be as sources and methods are compromised. Also, even if a state can successfully attribute an attack, it must convince its adversary of this fact, without compromising too much intelligence.

Libicki outlined various methods of attribution, but cautioned against “false flag” attacks. He urged that the U.S. consider the question, “Who benefits?” If word gets out that attribution is the main effort, then some actors could intentionally conduct an attack in a manner that frames another.

Deterring in a “Global Commons”

Pudas noted that many are referring to cyberspace as the “newest of the global commons,” but he argued this may not be the right model. In the final analysis, all cyber activity has a physical location, with computers and keyboards. Thus, geopolitical considerations and strategic calculus come into play.

Private Sector Involvement

The role of the private sector in deterrence—and in cyber security more generally—is both critical and complicated.

Pudas noted some policy and cultural impediments to cooperation. He said the private sector wants to collaborate with government, but does not want to risk adverse discovery and the litigation that it could entail. Due to fierce competition, companies fear losing market share if knowledge of an attack became public.

O’Neill put forward a more basic argument—that the U.S. must conceptualize threats in a way that accounts for private sector understanding and expertise, because “they deal in this world every minute of every day.” He also wondered how a company like Goldman Sachs—with US interests and Chinese interests as clients—would address deterrence. Dependency creates obstacles but also may be a way of creating a new form of deterrence.

Zeichner referenced the Troubled Asset Relief Program as a learning source. From a cyber perspective, he said, the very large corporations that form the backbone of the economy are “too big to fail.” Thus, it is important to think about how the U.S. might confer a benefit to very large corporations. Zeichner acknowledged such measures might not be fair, but were necessary.

Seriousness of Effort

A common theme throughout the panelists’ remarks was that the issue of deterrence requires a great deal of attention and demands considerable effort given the multitude of challenges that are present.

Pudas referenced the Estonian public awareness campaign, saying they “have it right.” In the U.S., “the average person on the street has not had the Estonian, life-changing experience.” He also noted that the U.S. sets new norms and thresholds every day it fails to take action.

Norms & Policy Guidance

The panelists all acknowledged that the U.S. needed to proactively develop norms and rules for conduct. In cyber, there is a concern that efforts to improve security will be interpreted as infringing on civil liberties and privacy. Nacht identified a need or policy guidance to know “what we should and shouldn’t be doing.” He also noted that Congress should be regularly informed of all activities.

LUNCHEON KEYNOTE: SUSAN COLLINS

INTRODUCED BY:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute

BIOGRAPHY:

Susan M. Collins; Ranking Member, Senate Committee on Homeland Security & Governmental Affairs

Maine voters first elected Susan M. Collins to represent them in the United States Senate in 1996. She was reelected in 2002 and 2008. She has earned a national reputation as a thoughtful, effective legislator, who works across party lines to seek consensus on our nation's most important issues.

Senator Collins is Ranking Member and former Chairman of the Homeland Security and Governmental Affairs Committee, which has jurisdiction over the Department of Homeland Security and is the Senate's chief oversight committee.

Senator Collins coauthored the Collins-Lieberman intelligence reform legislation, which was signed into law in December 2004. The law represents the most sweeping changes to our intelligence community in more than 50 years and implements many of the recommendations of the 9-11 Commission with a focus on improving our intelligence systems to help prevent future terrorist attacks.

Vulnerabilities in the Cyber Realm

Senator Collins began by discussing the escalation of threats to the security of national cyber infrastructure, noting that the internet, one of the most significant inventions in human history, enables as well as endangers vast amounts of activity that occur in cyberspace each day. She presented the sobering fact that cybercrime costs the US economy \$8 billion annually, while hackers can operate in relative safety and anonymity from almost any locale. Collins also discussed the potential that terrorists have to shut down the nation's power grid, critical infrastructure, and economic systems. The current system is vulnerable to these very real threats which highlight the priority U.S. policy makers must give to cyber security.

Current Cyber Situation

Collins stressed that, despite the ominous warning signs, the U.S. government has not done nearly enough to effectively secure most government IT systems. Due to the interconnectivity of these systems, a weakness in one area represents a potential vulnerability in all areas. She concluded, given the current situation, it is fair to ask whether or not the US will have to endure a "cyber 9/11" before the government acts to address these issues. The current laissez-faire attitude cannot continue; the government must move past the planning and start to make changes today.

Cyber Security Strategy Moving Forward

Senator Collins and Senator Joe Lieberman (I-CT) have focused much of their collective efforts on cyber security matters by holding three hearings on the issue. She discussed the need for a comprehensive cyber strategy that would allow for coordination among law enforcement, the military, the private sector and critical infrastructure. Finally, Collins discussed the potential development of a separate organization like the National Counter Terrorism Center (NCTC) as a model for cyber security. The NCTC plays a dual role, and she is convinced that a similarly-conceived cyber security center could play a dual role for public and private sector cyber security.

White House Involvement & Leadership from DHS

Collins also noted that although some experts suggest that the cyber security effort should be led by the White House, she has come to a different conclusion. This conclusion involves the need for aggressive oversight, testing, monitoring, and assessing of security threats which cannot be effectively managed by a small White House-based staff.

Instead, Collins proposed that the Department of Homeland Security (DHS) is the logical leader for cyber security. Nevertheless, a coordinated effort between the intelligence community, DHS, the White House and the National Security Council is vital in ensuring the security of the system day to day.

SESSION THREE – SOLUTIONS

From whence should we expect solutions to originate? What potential solutions for a balanced national strategy exist? Are there opportunities for cooperation? What new policies are needed?

MODERATOR:

Frank Cilluffo; Director, The George Washington University's Homeland Security Policy Institute

KEYNOTE:

Richard Barrett; Coordinator, Al-Qaeda Taliban Monitoring Team, United Nations

PANELISTS:

David Grannis; Majority Staff Director, Select Committee on Intelligence, US Senate

Neill Sciarrone; Former Special Assistant to the President for Homeland Security; Director, Cyber Security and Information Sharing, BAE Systems

Overview & Background

Richard Barrett's keynote and the ensuing panel discussion highlighted the critical role focal points of common understanding will play in the development of effective cyber solutions. Each of the speakers referenced the utility of such in describing the nature and meaning of threats – and in shaping what are to be deemed appropriate responses.

David Grannis and Neill Sciarrone argued that common focal points are critical to developing responses at the national and international level. Grannis and Sciarrone posited that such focal points play a critical role in developing the public-private partnerships necessary for effective solutions.

Barrett's comments, however, suggested that international focal points remain elusive; in large part because of the disparate levels of threat faced by various nation-states. Yet, Barrett stated that most countries do wish to establish international cooperation. He charged that the international community is looking to America for leadership – and now is the time for the US to decide just what it wants the rest of the world to do.

Terrorists' Use of Cyber

In his opening remarks, Richard Barrett stated that terrorists have not thus far used the internet in large scale attacks. Yet, he continued, they display an almost "nerdish" fascination with the internet and are heavily invested in it as a communicative tool.

Barrett noted that the internet has magnified the impact of terrorism – it has increased terrorists' ability to threaten and frighten, plan attacks, and train. As a result, he argued, when discussing efforts to reduce the presence of terrorists on the internet, it's a zero-sum game, at least for legitimate actors – terrorist are the only losers.

According to Barrett, most of the activity on terrorist internet sites is posted by a few key individuals. Identifying and arresting these small numbers can have a large effect – thus many governments, and even private actors, have established internet monitoring units.

Still, Barrett argued, the likelihood of a universal agreement banning terrorists from the internet is low. Barrett attributed this to the fact that most nations lack a terrorist cyber presence and reluctance on the part of internet service providers to police the web.

Issues That Shape Solutions

Barrett stated that the UN's *Working Group on Countering the Use of the Internet for Terrorist Purposes* had identified the following categories of issues as key in shaping solutions to cyber threats:

- political, which often coalesce around protections for freedom of speech;
- legal, which address definitions of criminal behavior and proper punishments;
- technical, which identify challenges in stopping or preventing illegal activities;
- financial, including the distribution of the costs associated with a given solution; and,
- civil society, which question whether solutions undermine cyber's benefits.

International Convergence & Divergence

In his keynote, Barrett noted that despite the presence of common issue categories and a widespread recognition of a need for public-private partnerships – national governments continue to experience great difficulty establishing areas of agreement and collaboration. He noted that most governments continue to deploy cyber solutions in a manner reflective of their specific culture and characteristics. According to Barrett, this condition stems from an increased perception that cyber security is increasingly tied to national security.

Barrett noted, however, that there has been some agreement – mainly in the restriction and prosecution of those trafficking in child pornography. Furthermore, Barrett noted the leading role taken by Russia in the development of international agreements.

According to Barrett, the UN found that some work is being done regarding how countries may best respond to and recover from cyber attacks. Yet, he noted, such efforts remain dependent on informal networks of key individuals.

Evaluating Opportunities & Risk

Sciarrone called for the development of metrics for evaluating the opportunity costs of potential policy choices. She noted that often security gains are traded for resulting losses in functionality.

Sciarrone stated that an enhanced ability to generate risk assessments was also needed. She argued that such assessments provide vital information regarding resource allocation.

Grannis noted the centrality of public awareness in developing solutions. He called for greater efforts to promote public understanding of the opportunities and risks that come with cyber – in illustrating the need, Grannis referenced campaigns promoting the use of seatbelts.

Standardized Efforts & a Common Lexicon

Grannis and Sciarrone highlighted the importance of standardized efforts in crafting cyber solutions. Grannis noted that this was important at both the national and international levels. He referenced the Pentagon's new cyber command, but worried that such effort would not be mirrored in other agencies – such as the State Department. For Grannis, this

raises concern about the coherence and consistency of US cyber policy.

Sciarrone argued for the establishment of a common lexicon. She noted that as cyber issues are engaged, one quickly learns that actors do not use the same terms – or worse yet, occasionally employ common terms with different meanings. In order to coordinate effective solutions, Sciarrone insisted a common lexicon was vital.

Crafting Response Mechanisms

Grannis stated that thus far legislative efforts have centered upon questions of jurisdictional organization. He noted that in the past year, Congressional committees and staff have increased their focus on cyber related issues.

Grannis pointed to the need to encourage cooperation among private sector actors, but noted that such might require granting protections from certain liability issues.

When asked by Frank Cilluffo about how legislative efforts might balance pushes for cyber solutions without stifling innovation, Grannis commented that history illustrates the importance of making sure laws written today do not hamstring future generations. Regulations need to maintain flexibility and at times benefits may be realized by leaving specific items out and avoiding legislative micro-management.

Playbooks

During the panel discussion, Sciarrone referenced the playbooks that many government agencies and departments maintain for what to do during a natural disaster. She suggested similar guides be developed for various types of cyber events. Such playbooks would provide operational instructions, menus of options, and lines of responsibility. Although each of these playbooks should be tailored to their respective agency, Sciarrone insisted they must be coordinated at the presidential level.

SESSION FOUR – IMPLEMENTATION

How can the U.S. best implement potential policy solutions? How should cyber deterrence be coordinated—both within government and between governments and private industry? Where and how can governmental resources address key cyber challenges? What are the best methods for evaluating successful implementation of policies?

MODERATOR:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute

KEYNOTE:

Philip Reiting; Deputy Undersecretary for the National Protection and Programs Directorate, Department of Homeland Security

PANELISTS:

Steve Chabinsky; Deputy Assistant Director, FBI Cyber Division

Jeff Cooper; Vice President for Technology, SAIC

Thom Shanker; Correspondent, The New York Times

Suzanne Spaulding; Principal, Bingham Consulting Group

Overview & Background

The keynote and panel discussion built upon the outcomes of the “Solutions” panel and included much unique insight into the thinking, capabilities, and potential actions of government actors.

Roles & Responsibilities

Philip Reiting began the discussion with a call to build out the “foundations of work” in the federal government. Collective responsibility should provide a model for bringing together all national resources. Agencies across government must have clear roles and responsibilities. Like a soccer team, each has positions to play, and must learn them and play them well.

One important facet of this approach is to develop a cyber incident response plan—a “playbook” of what to do in various circumstances. Most importantly, the playbook should be an extension of natural day-to-day operations, because individuals in crisis do what they normally do, albeit scaled to meet the emergency.

Steve Chabinsky reiterated the necessity for collaboration and stressed the need to identify

partners that could help reduce the threat by lowering vulnerability and the adversary’s probability of success. Thom Shanker added that it is still not clear to the military what its role would be in responding to a cyber attack.

Building Organizational Capabilities

Besides having a plan, Reiting argued that it was crucial that the necessary actors have the capabilities and capacity to execute their missions. Suzanne Spaulding noted the importance of the convergence of human and technical means—a direction toward which the Director of National Intelligence is moving.

Affecting the Opponent’s Decisionmaking

Picking up on the practicalities of implementing a deterrent strategy, Jeff Cooper noted that deterrence can be effective even if the target is unknown, because it still affects the decisionmaking processes of potential adversaries. For Cooper, the first element in supporting deterrence is lowering or limiting the probability of the adversary’s success. Chabinsky characterized the challenge as one where the US looks to affect the cost-benefit calculus of the adversary. In either case, an adversary’s appreciation for a target’s warning and safeguard capabilities will factor into whether or not that opponent will be deterred from attacking.

Warning

Chabinsky focused on warning as a critical element of the implementation process. In relation to the discussion on roles, he suggested sharing warning of an attack to various interested parties so that they could provide assessments of what the threat means to them specifically. He noted that there are numerous examples of the government recognizing a threat and attack before the private sector, or vice versa.

Who the adversary is factors heavily into warning. Spaulding highlighted counterintelligence as an effective and important aid in warning, because it helps to prioritize responses to threats and actions. Chabinsky added that it’s also important to evaluate who the adversary is and who the potential victim is when considering warning. Depending on whether or not the victim has the ability to protect themselves, warning could end up doing more harm than good if it supplies the adversary with additional useful information to launch an attack.

Safeguards & Defense

Cooper broke down three key elements of security, each with their own characteristics and requirements: 1) protect infrastructure and transportation systems; 2) protect cyber domains; and 3) protect public access.

He also described a new defensive paradigm that differs from the Cold War era concept of nuclear deterrence. At that time, deterrence was based on a two-party, two-state paradigm, said Cooper. This mindset is no longer applicable. Instead, defense must be operational in nature, not static. Defenses ought to force the enemy to disclose identity and intent. Cooper's criticism of the United States' current posture was that it remains quite static and lacks heterogeneity.

Reitingner approached defense from a resiliency angle, arguing that the ability to bounce back is key. "The status quo is not sufficient. We have an ecosystem right now where the attacker wins...and that is not sustainable." He also argued that defense cannot just be about information sharing, which in and of itself does not accomplish anything.

Culture & Approach

Cooper stressed the importance of being cognizant of the technology being used, just as it is important to recognize the dangers of operating a car. Cooper challenged the conception of looking at cyber as if it were the high seas, which misses the fact that cyberspace is created by physical machines that exist in real places. Thus, it is important for the United States to consider how it exerts sovereignty, and how it might enforce responsibility for what occurs in other actors' areas of sovereign control.

Shanker brought up the notion that the US is too focused on a firewall and on defense, and is not spending enough time on offensive elements and emphasizing its offense capability, which is something the military thinks about. He also added that US leadership has failed to engage the American public in the cyber debate. As a result the American public is not prepared, because we have not had the discussion about why cyber is important and what we ought to be ready to give up in exchange for security.

Spaulding echoed Shanker's call for more open, public debate on the issue, but also brought up the value of counterintelligence as an approach to cyber security and deterrence. Spaulding suggested that counterintelligence would provide insight into an adversary's overall strategic goal, as well as their knowledge and misunderstandings about the US. Counterintelligence would also help the US to exploit an adversary's vulnerability where the human meets the machine.

Spaulding also pointed out the necessity to broaden the U.S. approach to cyber, so that we no longer think of responding to cyber events with strictly cyber-based actions. Finally, she said that US strategy cannot be based on secret information. Instead, the US should be with the "Linuxes of the world" and the "football coaches who put their playbooks online." Her bottom line: proprietary information is irrelevant because the US should be innovating at a rate that renders public knowledge of secrets inconsequential.

Legal Implications

Shanker and Spaulding also touched on some of the legal issues of implementing a cyber deterrence strategy. Shanker asserted that the laws of war have yet to catch up with the cyber domain. He posed several hypothetical issues for consideration, including: what if you turn off the electrical grid and a hospital sits on that grid? and what is the military commander's responsibility for responding to attacks that venture through third-party, perhaps neutral countries?

Spaulding put the onus on policymakers to identify goals and objectives in the cyber arena, then develop strategies which lawyers—and if necessary, Congress—can evaluate. She indicated that questions concerning what constitutes use of force in cyberspace may not be the best questions to ask. What is important to explore, she argued, is why we would ask these questions and why we would care.

PRESENTATION OF INSA CYBER TASK FORCE PAPER: “ADDRESSING CYBER SECURITY THROUGH PUBLIC- PRIVATE PARTNERSHIPS”

INTRODUCED BY:

Ellen McCarthy; President, Intelligence and National Security Alliance (INSA)

PANELISTS:

Lou Von Thayer; President, General Dynamics Advanced Information Systems

Steve Cambone; President, Mission Solutions Group, QinetiQ-North America

Barbara Fast; Vice President, Cyber Solutions for Intelligence and Security Systems, Boeing

Charlie Allen; Steering Committee Member, Homeland Security Policy Institute; Senior Intelligence Advisor, INSA

Robert Gourley; Founder and CTO, Crucial Point

John Russack; Director, Intelligence Community, Northrop Grumman

Robert Farrell; President & CEO, Seneca Technology Group

Overview & Background

Lou Von Thayer provided a review of INSA’s task force paper: “Addressing Cyber Security Through Public-Private Partnerships.” Von Thayer stated that the INSA task force had developed a model for public-private partnership to address cyber issues after viewing the use of such partnerships in other issue areas.

Von Thayer argued that because of the unique nature of cyber, no previous model provided a complete solution – however, several models offered beneficial elements. Von Thayer stated that INSA had selected a hybrid model exhibiting private sector leadership with governmental support. The model would create a cyber security panel that, according to Von Thayer, would make recommendations to a governing body. The logic of private sector leadership was highlighted by John Russack. Russack stated that more than eight-five percent of cyber infrastructure is in private hands.

Incentives Rather than Regulations

Lou Von Thayer stated that the task force was motivated by questions concerning how to get actors to participate and how to develop reasonable standards.

Barbara Fast commented that in searching for a model the task force realized that the focus had to be on incentives – on “carrots rather than sticks.”

Steve Cambone noted that the mechanism being suggested was one in which private sector actors would approach government with a clear idea of what was needed. Cambone compared the model to a social network and noted that the model depends upon the participation of those being regulated. Similar to the relationship between the FAA and airlines, Cambone suggested. John Russack explained that the cyber security panel would identify areas where greater collaboration was needed and then approach the government for support in incentivizing collaboration.

Domestic Before International Emphasis

The panel recognized the international dynamic of cyber. Lou Von Thayer expressed the belief that eventually there would be an international component; however, he stressed the need for American actors to focus on the development of domestic processes first.

Bob Gourley insisted that the panel understood the need for global standards. Yet, Gourley commented that INSA’s recommended cyber security panel would not provide such. Nonetheless, Gourley pressed for the need to support the development of private-public partnership within the United States.

For his part, Steve Cambone argued that the US may have, as a country, missed its chance to set the global standard and that the US lacked the dominance to do so today.

Dynamic Framework

The panelists suggested that the framework being presented was intended to provide a dynamic forum for solving cyber challenges. Lou Von Thayer stated that he could see the group proposing minimum standards. Bob Gourley said he believed the group could help both develop common audit guidelines and implement common practice.

Charlie Allen said the model had enough agility to work from the bottom up and factor in various elements of American society and the federal government.

CLOSING KEYNOTE: CHRIS PAINTER

INTRODUCED BY:

Frank Cilluffo; Director, The George Washington University Homeland Security Policy Institute

BIOGRAPHY:

Chris Painter; Acting Senior Director of Cybersecurity, National Security Council.

A leader in cybercrime and cybersecurity issues since the early 1990s, Painter was part of the team that wrote the President's 60-Day Cyberspace Review.

From 1991-2000, Painter worked as a Federal Prosecutor in Los Angeles specializing in high profile computer crimes – including the prosecution of notorious computer hacker Kevin Mitnick and prosecution of the “mafia-boy” distributed denial of service case that involved attacks on Yahoo!, Ebay, CNN, and e-commerce sites.

From 2000-2008, Painter helped lead the Department of Justice's Computer Crime and Intellectual Property Section.

Painter has chaired the G8's High Tech Crime Group for nearly eight years. In that role, Painter expanded that organization's High Tech Crime Point of Contact Network to more than 50 countries. During his tenure he also chaired a high level meeting on Critical Information Infrastructure Protection (CIIP) that resulted in a set of foundational CIIP Principles that were adopted by the United Nations General Assembly.

Painter has served as the co-chair of the National Cyber Response Coordination Group and is a founding member of the National Cyber Study Group.

Nature of the Cyber Threat

Chris Painter began his keynote remarks by referencing President Obama's speech of May 2009, in which the President noted that the very technologies that support our economy can be used against it.

Furthermore, Painter argued that we face a broad spectrum of integrated cyber threats. He emphasized the fact that cyber threats possess an inherently dynamic nature. Each year, said Painter, we witness new, more clever, forms of attack.

Cyber Security

According to Painter, cyber security must be about more than hardening targets. He stressed the need to incorporate strategy, policy, standards of security, and operations. Security efforts, he said, should draw upon law enforcement, diplomacy, military, and other national resources.

Deterrence

Painter stated that deterrence can act as a great organizing principle. He pointed out that deterrence activities include prevention, resilience, and response.

However, Painter was clear that deterrence is ultimately about raising the costs and consequences to an adversary. For that, he argued, we need to foster cooperation that facilitates response capabilities.

Whole of Government Responses

Painter stated that one the most important issues facing the government is the need for interagency cooperation. What is needed is a willingness to contribute and deliver. Painter stated that the government must find a way to coordinate and harness the capabilities and responsibilities of each agency.

Whole of Society Responses

Although government will play a key role, Painter's comments made it clear that addressing cyber issues requires a whole of society response.

Painter noted the importance of individual awareness and cited the President's National Cyber Security Awareness Month (October 2009) video calling on citizens to protect themselves in the cyber realm.

He also highlighted the importance of addressing questions regarding civil rights and civil liberties, as well as the need to define legal thresholds concerning “use of force” and cyber self-defense.

Painter referenced the key role to be played by the private sector. Painter called for research investments into “game changing” technologies and called for security protocols to be “baked in” rather than layered on afterward.