

## Conference Summary: Strengthening Homeland Cyber Defense

**Erin Schlather  
Joelle Laszlo  
Kristen Batch**

*This summary was prepared using tapes, transcripts, and other materials from the conference. It is meant to provide an overview of the event, though some of the views presented are not necessarily shared by all of the conference speakers and participants.*

On October 18<sup>th</sup>, the Center for Strategic and International Studies (CSIS) and the Information Technology Association of America (ITAA) held a half-day conference to examine Homeland Cyber Defense in light of the events on September 11, 2001. The first half of the conference featured remarks from (in this order): John Hamre, President of CSIS; Harris Miller, President of ITAA; Ronald Dick, Director of the National Infrastructure Protection Center; Duane Andrews, Executive Vice President of Science Applications International Corporation; and U.S. Senator Robert Bennett (R-UT). The second half focused on the industry's perspective, with a panel of executives offering their thoughts on protecting critical infrastructures and John Tritak, Director of the Critical Infrastructure Assurance Office chairing the discussion.

The conference was premised on the fact that the terrorist attacks of September 11<sup>th</sup> have inexorably changed the way our nation and leaders think about homeland defense. The speakers and panelists conveyed the sense that, as John Tritak noted, it is not the urgency of effective cyberdefense that has changed, but rather the appreciation of that urgency. In addition to the massive response by the government to the physical vulnerabilities of the homeland, it is crucial that similar attention and resources be allocated to addressing the vulnerabilities of our critical infrastructure to a cyberattack.

Dr. Hamre opened the conference by applauding the rush of enthusiasm for securing cyberspace since the September 11<sup>th</sup> attacks. He observed that the Internet's infrastructure was built over the years without enough forward planning for security and safety. With the threat of a terrorist attack now tangible, there is an increasing commitment to fireproofing cyberspace both at home and abroad. Dr. Hamre expressed optimism that such efforts will be sustained due to the personal investment that both the private and public sector have in securing their infrastructure.

In addition to this commitment to increase cybersecurity, Dr. Hamre noted that important advances will be made in various technologies, including biotechnology, due to the resources invested by the government and the private sector since the attacks on September 11<sup>th</sup>. This moment of crisis may, in fact, lead to critical breakthroughs in science and technology over the next five years that will be of an enormous benefit to society.

Harris Miller then outlined the themes of the conference: 1) there must be increased cooperation between government and industry; 2) the government must invest the

necessary resources to upgrade and secure its own systems so as to lead this effort against terrorism; 3) resources must be put into educating businesses and government about the realities of cybersecurity; and 4) international cooperation must be reinforced through government action.

In his remarks, Miller emphasized the improvements that have taken place in the past few years, both in the private sector and in the government. The number of Information Sharing Analyses Centers (ISAC) that coordinate information sharing within specific industries and the government have increased over the past few years and are becoming more effective. Interagency organization and cooperation are improving through actions such as the establishment of the President's Critical Infrastructure Protection Board and the appointment of Dick Clarke as the new Information Security Czar.

However, the federal government must take greater steps in protecting its own critical infrastructure. Every government agency must have upgraded systems, as should both state and local governments. More money must be invested into information security research and into the training of information security workers. Together, government and industry must educate small and medium sized business about the importance of solutions through people and process, not just through technology. While these actions will require a substantial financial investment by the federal government, Miller maintains that it is absolutely necessary in the fight against terrorism and in protecting the nation's financial and physical security.

Finally, Miller called for increased international collaboration. While applauding the Council of Europe Cyber Crime Convention for attempting to establish a baseline for international standards in dealing with cybercrime, Miller maintains that the process taken for the convention was ineffective. There should be a more effective coordinating mechanism internationally, and it must reach all countries, much like the Y2K coordinating agency did in the late 1990s and in 2000.

Ron Dick, Director of the National Information Protection Center (NIPC), echoed many of Harris Miller's sentiments including increased collaboration between the public and private sectors and within the international community. The NIPC, he said, is an important mechanism for such cooperation, but should not be the only vehicle for information sharing. The NIPC serves to respond to threats by protecting the government's critical infrastructure through early detection of threats and vulnerabilities. They then assess the threats and warn the government and the private sector in a timely fashion, while simultaneously formulating a response to the perpetrators of the crime.

In addition to this agenda, the NIPC also focuses on strategic analysis as a critical element for effective protection. The goal is to be able to forecast threats with enough time to prevent them, to reduce vulnerabilities through education, and to mitigate the free flow of information between government agencies and the private industry to increase detection capabilities and minimize damage after an attack occurs.

To accomplish this, according to Dick, NIPC ensures that proprietary information can be transferred between industries and government in a confidential manner. He cited the Code Red worm as an example of effective collaboration between the private and the public sector to deal with a serious threat. This collaboration was strengthened by the events of September 11<sup>th</sup>. In an effort to heighten security, information sharing among various ISACs (financial, electrical power, and others) has increased tremendously, as has their cooperation with NIPC, which is providing critical information from FBI investigations.

Duane Andrews, Executive Vice President of SAIC, made a stronger case for strengthening the government's defenses to a cyberattack. He claimed that the lack of decisiveness on the part of the government and industry to protect against cybercrime before now was because a) cybersecurity is technically complex and hard to understand; b) every dollar that would go into protection and reaction is a dollar out of another budget; c) there are no mechanisms to make government or industry accountable; and d) cybercrime has always been treated as a tactical problem, rather than a strategic one. According to Andrews, that can no longer be the case and terrorism, in any form, must be treated as an act of war, rather than as a criminal act that can be dealt with in a court of law.

Andrews again emphasized the need for continued education for government and industry on the importance of cybersecurity and the sharing of know-how. Businesses, particularly small and medium sized businesses, are more concerned with the insider threat to their security, and while that is an area that should be dealt with, resources must be invested into all facets of cybersecurity protection. Further, Andrews reiterated the need for the government to invest in even the most basic steps in solving the cybersecurity problem. Sound system designs, strong system administration, and improved security training for personnel are among the most basic steps that have to be taken. Most of all, Andrews claimed, there must be a mechanism for accountability that will place the responsibility of an attack on those that have the influence to make the changes necessary to protect against future attacks.

The first half of the conference concluded with remarks from Senator Bennett, who along with U.S. Senator John Kyl (R-AZ) has drafted legislation that specifically responds to the cyberthreat to homeland defense. The legislation removes some barriers to information sharing between the private sector and government about both cyber and physical vulnerabilities. With over ninety percent of the of the country's critical infrastructure owned and/or operated by the private sector, information sharing between the government and industry is vital.

The Bennett-Kyl bill, S. 1456, emphasizes communication between government and industry, and between different areas of industry. Such information sharing is crucial to identifying possible patterns in cyber disruptions across various sectors that would indicate a coordinated terrorist attack. S. 1456 (as well as a House version (H.R. 2435), co-sponsored by U.S. Representative Tom Davis (R-VA) and Jim Moran (D-VA)) allows for such a dialogue between corporations and industries to take place without the pressure

of antitrust laws. Further, the bill would clarify existing Freedom of Information Act (FOIA) language so that the intelligence can be shared with the government, without the fear that it will enter the public domain. (In absence of clarification on this point, corporate counsels currently advise their clients not to share voluntarily the details of computer attacks and other cyber and physical vulnerabilities with government agencies. In their judgment, the risk that such data could ultimately be divulged through a FOIA lawsuit – even over the agency’s objections – is unacceptably high.)

Senator Bennett also emphasized the need for an oversight mechanism akin to the Y2K initiative. The back-ups that were put into place during the millennium contributed significantly to the ability of the financial sector to jump back so quickly from the September 11 attacks. Similar mechanisms should be ongoing for the protection of all critical infrastructures, across industry sectors and government.

### **The Private Sector and Homeland Cyberdefense**

John Tritak, Director of the Critical Infrastructure Assurance Office (CIAO), provided the opening comments for the second half of the Homeland Cyber Defense conference and introduced the panel comprised of leading industry experts in the area of cybersecurity. Tritak first clarified the relation between critical infrastructure protection (CIP) and homeland security. He indicated that CIP is just one aspect of homeland security, and that the necessity of cyberdefense is not limited to only the protection of the national infrastructure, since this necessity extends to all parts of our society and our economy. Long before September 11, the CIAO has made the case that cybersecurity makes good business sense. However, since this date there has been an increased awareness that national security is an industry concern. Tritak stressed that a reliance on our infrastructures exists for industry to run their businesses, for the Federal Government to carry out its functions, and for the general public to access and receive services to conduct their daily lives.

Tritak reiterated the steps that the Federal Government is taking to protect against a cyberattack, but stressed that defense of the homeland, in all of its dimensions, cannot be done by the Federal Government alone. It requires a collaborative effort, which must be achieved through public-private partnerships. The government can facilitate market solutions that can help to support and secure the nation’s infrastructure, such as safeguarding information sharing between the private sector and the government. The private sector can offer expertise to work toward solutions to safeguard our critical infrastructure.

During his opening remarks, Tritak also expressed the Bush Administration's support for a “narrow FOIA exemption.”

Steve Blumenthal, Senior Vice President and CTO of Genuity, discussed the need to understand the infrastructure of the Internet to identify where the security risks can take

place. He touched on three areas: peering points, types of cyberattacks, and software diversity.

Industry has greatly increased the number of private peering points. This level of redundancy helps to ensure the functioning of the Internet, even if critical connection points were taken down. This is not the case for many smaller ISPs which are directly connected to the Internet through a fewer number of public peering points. The services provided by smaller ISPs might fail, if the public peering points are taken out.

Other critical areas include corruption of Domain Name Systems (DNS) code or distributed denial of service attacks, in which too many coordinated hits to a particular web site render it inoperable. Solutions to these problems include work with digital certificates to prevent non-authorized manipulation of domain names and firewalls and filtering algorithms to prevent against denial of service attacks.

A third vulnerable area is the infrastructure software used to run everything from email to routers. Blumenthal said that without greater software diversity, viruses have more ability to take down more service providers at once.

Industry can play a large role in finding and working toward solutions for the problems identified in the above three areas. Government must also play a role in sponsoring more R&D through DARPA and should continue exploring the idea of a 'GOVNET' to secure intra-government Internet traffic.

George Conrades, Chairman and CEO of Akamai, emphasizes the need for critical infrastructure improvements, by shifting away from Border Gate Protocols (BGP) to distributive computing that can help prevent against many of the physical and cyberattacks outlined above. Conrades identified the central weakness of the Internet infrastructure and the lack of security aspects in the basic design of the 7,000 networks that comprise the Internet. Through the use of the existing BGP, it is not possible to know who is sending messages and from where the messages are being sent. Conrades highlighted the alternative of distributive computing, which functions as an overlay network to the Internet by moving the contents of websites to their servers. With the ability to monitor the origin and IP address of the sender, they are able to protect against many attacks, such as cyber hijacking and code corruption of DNS servers.

David Langstaff, CEO of the Veridian Corporation, then spoke on the importance of putting communication and coordination with the federal government in areas of cybercrime. He emphasized the need for every corporation to be coordinated with each other in this effort and for the challenge to be on the agenda of every CEO. Mr. Langstaff said that over 95 percent of the Internet is owned by private industry so it is crucial that the government develop a new legal structure that will allow for increased information sharing both within the private sector and between the private sector and government. Such a structure would have to remove the current barriers to information sharing, such as existing FOIA language. Finally, Langstaff restated the need for the government to invest more resources and funds into fighting this very viable threat.

Gail Phipps, Executive Vice President of CACI International began her remarks by suggesting a cyber-Federal Emergency Management Agency, to act as an oversight mechanism for dealing with cybercrime. Such an agency would develop a cyber emergency response plan. In addition to improving this kind of institutional response, Phipps suggested that protections such as firewalls should be put into every piece of software and on every PC. Phipps said that these types of aggressive actions are needed to manage the continuing risk in cyberspace.

Finally, Dr. Ernst Volgenau, President and CEO of SRA International, concluded the panel by reemphasizing the vulnerabilities that exists in our homeland to a cyberattack. All of the major industries have central hubs that face a real threat and would seriously disrupt society if attacked. Further, the government's response does not include any sort of back up, so if something were to happen to one of those agencies, no redundancy exists to ensure the constant flow of information.

### **Themes and Recommendations**

Though they took different routes, the individuals who spoke at the conference arrived at essentially the same conclusion: in order to strengthen homeland cyberdefense, we must change the way we think about network security, and use this awareness to motivate a solution. We have a fairly good sense of what the risks are, and plans in place for mitigating those risks. Now we need to set clear, tangible goals with concrete timelines and move forward. We need to be able to identify our progress toward security just as clearly as we can now identify our vulnerability. At the same time, we must remain serious about the importance of cybersecurity, and the implications of a failure to effectively defend the nation's critical infrastructure. Complacency is no longer an option.

#### **Thinking About Cybersecurity**

We've known for at least a decade that the country's critical infrastructure depends on computer systems and information networks that are subject to debilitating cyberattacks. But until now, network attacks have been more burdensome than anything, and costly for only a handful. The unthinkable events of September 11, 2001 removed the illusion that anything is unthinkable.

In this new environment, the denial of service attacks that we face today should be likened to the failed World Trade Center bombing of 1993 – a mere harbinger for a future strike that devastatingly succeeds. At least, this is the idea that the conference panelists promoted. There has long been a disconnect between the recognition of the cyberthreat and the allocation of resources to manage it. High-level officials from the public and private sectors have discussed the issue in countless meetings, even strategized over possible defenses. And yet year upon year, the number of attacks grows, while cyberdefense budgets remain pitifully low. Cybersecurity needs to be a management

priority in both the private and public sectors. The nation's critical infrastructure is subject to a terrorist or military strike. Homeland defense, and all of its components, is a business concern. Network security cannot be left only to information technology departments and technical staffs; management must be held accountable.

At the same time that critical infrastructure protection must be given greater appreciation at executive levels, it must also be reconsidered as a tactical issue and not just a strategic one. Up to this point, most CIP discussions have focused on one-dimensional cases, like the damage that a virus could wreak when launched against the power grid in a major city, or several cities at once. But according to Senator Bennett and others, this way of thinking prevents us from realizing just how dangerous – and costly – a cyberattack can be. The emergency rescue personnel that raced to the World Trade Center were working off of an established response plan that required clear communications among dispatch offices, crews in headquarters or en route, and those already on the scene. Had something gone wrong in these communications, surely countless more would have perished. Cyberattacks are currently imagined as independent “virtual” events that have physical consequences and require physical responses: for example, strikes against computers at purification plants that send unsafe drinking water into the pipes of consumers. It's time we turn this vision around, and realize that the mobilization of physical responses to individual physical attacks depends on cyber networks. And then imagine the horror of an event that involved simultaneous physical and cyber strikes.

### **Building Effective Cyberdefenses**

With a clear conception of the need for cyberdefenses, the creation of those defenses can move forward. More accurately, once the threat is completely understood, the resources for effective network security will more readily be allocated. Those resources include technology and money, people and laws, and most important but not as tangible, cooperation. Though nearly all of the nation's critical infrastructure is owned and operated by the private sector, the Federal government is the only entity capable of coordinating the CIP efforts of so many companies, organizations, and institutions. Thus, collaboration between industry and government is key to any comprehensive and effective cybersecurity strategy.

This point was raised again and again by speakers at the conference, and indeed no one doubts its validity. But public-private cooperation in cyberdefense has been slow in coming, a point that was just as clear to panelists and participants. With no need to dwell on it, attention was shifted to an example of successful partnering: the Y2K initiative of a few years ago. As the final months of the last century ticked away, government and industry worked together to solve the technical problems of Y2K. And they solved them. The effort was greatly proactive, yet also motivated by circumstance: everyone knew that the year 2000 was coming; everyone knew they had a deadline for action. We should think of cybersecurity in the same way. The nation's critical infrastructure will come under attack, we just don't know when.

This problem is solved by having a response plan in place long before it is needed. In order to fashion an effective response, it is important to realize several basic things about defending critical infrastructure networks. First, as with any defense operation, it is simply not enough to have intelligence. Analysis is key, and analysis based on data aggregated from a number of sources is even better. Hence, any cyberdefense initiative should include facilities for sharing information, within industry groups, within the government, and between the public and private sectors. And to ensure that these facilities can actually operate, legal barriers to information sharing (within industries and between industry and government) should be removed. Second, critical infrastructure systems and networks are susceptible not only to cyberattacks, but physical strikes as well. The first computer bug was indeed a bug (a moth, to be exact). For a CIP plan to be truly comprehensive, it must envision and incorporate responses to physical attacks. Third, people matter just as much as, if not more than, technology when security is at stake. Hackers constantly write and update code to exploit software vulnerabilities; old patches cannot defend against new viruses. But people who understand security, and who receive regular instruction, can adapt their skills to counter new attack methods. Finally, cyberdefense is expensive. Security requires an investment in highly sophisticated tools and training, which need to be regularly updated and improved because of the evolution and complexity of cyberthreats. To paraphrase Senator Bennett, every entity involved in homeland cyberdefense must undergo a “fairly significant paradigm shift in attitude” with respect to the costs of critical infrastructure protection.

The above considerations are geared toward fashioning a plan to prevent cyberattacks. But a complete response must also include strategies for short- and long- term recovery. It must envision, for example, the existence of redundant networks and systems to back up those that may be damaged or destroyed in an attack. It must include plans for bringing downed systems back online as quickly as possible, and for analyzing why defenses failed. It should also contain provisions for investigating cyberattacks and apprehending and punishing those that mount them. In this area more than any other, international cooperation is exceedingly important. Most of the significant cyberattacks launched against U.S. interests have either come from abroad or been routed through overseas networks. Other countries with a technology-based infrastructure like that in the U.S. can also expect to face cyberthreats from abroad. We thus share a common interest in moving early to prevent international cybercriminals from succeeding, and global cybercrime from advancing.

## **Recommendations**

From these shared beliefs and conclusions, a number of different recommendations emerged. At base, the recommendations are designed to set up the components of a comprehensive cyberdefense response plan as outlined above. That is, they call for greater cooperation, more money, more people, and better enforcement of current laws. But from that common ground, several very specific ideas were advanced. Some are included in the proposals below.

- ***Expand opportunities for information sharing.*** Information sharing and analysis centers (ISACs) must be established immediately in the critical infrastructure sectors where they are not yet present. Public-private information sharing must also be expanded (possibly through facilities modeled after the FBI's successful InfraGard program). Finally, existing legal barriers to industry cooperation (*e.g.*, antitrust laws), and to industry-government cooperation (*e.g.*, the Freedom of Information Act) must be redressed.
- ***Increase awareness of critical infrastructure threats and defenses.*** The physical threat to critical infrastructure networks has not been sufficiently explored, and must be if we are to fully comprehend CIP. Neither can we assume that we have pinpointed all of the cyberthreats to critical infrastructure. CIP must be considered a task of the highest priority, and treated as such. We should stop assuming that strikes against critical networks will be strategic, and consider the possibilities if they are tactically combined with physical attacks.
- ***Increase spending on cyberdefense.*** A truly comprehensive and effective plan will require the outlay of more money than ever before on cyberdefense. Government and private sector organizations must realize that this is not a "fail and fix" problem. Recovering from cyberattacks will always be more expensive than preparing for them; budgetary sacrifices in the name of prevention are necessary. The Federal government spent an estimated \$3 billion to address the Y2K crisis. It should spend at least that amount, and probably much more, on cyberdefense.
- ***Increase training and education for individuals on the front lines of cyberdefense.*** Government (and industry, but to a much lesser extent) faces the possibility of a near-term dearth of qualified technical staff to fill its cyberdefense needs. Proposals to provide education subsidies to or forgive student loan debts of future government technical workers should be reexamined and revived. Continuous training should be used as an incentive not only for bringing in new staff, but also for keeping government cyberdefense employees in their jobs.
- ***Establish response and recovery assets and procedures to ensure critical infrastructure attack survivability.*** The successful response to and recovery from a critical infrastructure attack depends on the ability to ensure the continued functioning of the networks that are hit. Thus, a certain redundancy of systems is required, up to and including the creation of wholly separate networks for crucial government functions (*e.g.*, the proposed GOVNET). It is also worthwhile to consider the establishment of a separate Federal Emergency Management Agency (or perhaps a new bureau in the current one) to specifically address cyberattack response and recovery.
- ***Coordinate internationally to facilitate the investigation and punishment of cybercrimes.*** Critical infrastructure protection is not now nor will it ever be a security concern solely of the United States. Any nation that depends on the

efficient functioning of domestic or global cybernetworks has a stake in CIP. International coordination of cybercrime laws and cross-border sharing of information on threats and attacks is crucial to stemming the global expansion of cybercrime.