

# Strategic Cyber Risk and Response Conference: Options to Enhance Cybersecurity

## Final Report

### A. Introduction.

This white paper briefly summarizes the insights that were developed during the course of the Strategic Cyber Risk and Response Conference. The Conference was conducted at the National Defense University (NDU), Fort McNair, Washington, DC on January 22, 2009. The conference was co-sponsored by the Center for Technology and National Security Policy (CTNSP), NDU, and the George Mason University (GMU) International Cyber Center. The conference attracted approximately 100 participants from government, industry, academia, and not-for-profits.

The conference was held under “Chatham Rules”. Thus, this paper does not explicitly attribute specific insights to specific presenters, panelists, or participants.

As context for the event, two products were circulated to the participants. First, an article was disseminated that briefly summarized the twelve unclassified items of the Comprehensive National Cybersecurity Initiative (CNCI). Second, the Executive Summary and Recommendations from a recent Center for Strategic and International Studies (CSIS) study on cyber policy were distributed. (That product can be obtained through the following URL: <http://www.csis.org/>.) Many of those comments were stated during the conference. The material from both the CNCI and the CSIS study is summarized in Appendix A.

In addition, the panelists and speakers identified a range of cyber recommendations for the next Administration. Several of those recommendations are summarized in Appendix B. Furthermore, the World Information Technology and Services Alliance (WITSA) conducted a meeting on December 2, 2008, in Hyderabad, India. For information purposes, their cyber security principles are summarized in Appendix C.

In view of “Chatham Rules” the specific panelists and speakers will not be cited specifically in this white paper. However, it is worth noting that the panelists and speakers came from government, industry, academia, and not-for-profits.

In the area of government, the speakers came from the Department of Defense (DoD), the Department of Homeland Security (DHS), Department of Commerce (DoC), and various intelligence agencies. The industrial participants included representatives from McAfee, Juniper, and CSC. The academic participants included senior staff from the University of Virginia and GMU. Finally, in the area of not-for-profits, the speakers were selected from CSIS, the SANS Institute, and the U.S. Cyber Consequences Unit (USCCU).

## B. Nature of the Problem

During the course of the conference, the nature of the cyber problem became increasingly clear. It was observed that the cyber problem is highly complex and time-varying. Given the number of organizations involved in the problem, it was noted that it has “many seams.” One of the participants noted that we confront a “wicked problem”. Wicked problems are generally viewed as being ill-posed (from an analysis perspective). In general it requires constant iteration between the totality of the problem and the individual components. Another panelist observed that the loss of cyber intellectual property can adversely affect economic and national security. In general, there was agreement that we face a serious, national security crisis.

Although the conference was divided among five panels, it soon became apparent that many of the panelists identified a variety of themes that cut across the individual panel themes. Consequently, this white paper identifies and discusses nine key themes that emerged during the course of the conference.

## C. Theme: Leadership.

The major theme that emerged from the conference was the need for strong, innovative leadership on cyber issues. One of the concepts that was discussed was the need for a Cyber Czar and strong support from the White House. In particular, leadership is needed to push information-sharing forward (see below).

There was broad consensus that the key to mitigation is leadership and information sharing. It was concluded that we can't stop compromises or intrusions, but we have to prepare for them. In addition, we need to come up with a common mitigation plan for a broad audience.

One of the panelists urged us to “keep it simple!” This required four inter-related activities: Plan, Lead, Organize, Act!

In addition, it was stated that **trust** is an important element of that leadership. Many of the themes that emerged sought to build trust between the public and private sectors. For example, one of the panelists noted that industry needs to be able to call Law Enforcement if there is a problem ... and expect to have them call back.

## D. Theme: Risk Management

The second major theme of the workshop dealt with the challenges of risk management. One of the panelists observed that today, risk management is done “in stove-pipes”. It was stated strongly that if risk management is to be performed effectively, it must be scoped very broadly, from an enterprise-wide perspective. To implement that concept, we must use contemporary economic thinking and tools.

During the course of the conference, several thoughts were articulated that related to risk management. First, it was stated that “cyber is more than computers!” Thus, one has to deal with the full range of cyber products (e.g., cell phones, FAXes). Second, it was observed that partial success is **no** success. Since adversaries face a “target rich environment”, they only need to be successful in a small percentage

of their exploits. Overall, it was appreciated that we “can’t stop intrusions” and we need to go beyond *ad hoc* responses to those intrusions.

The challenge facing the community is to reduce risk and allow the mission to be accomplished. Consistent with that philosophy, efforts should focus on reducing consequences rather than reducing vulnerabilities. As a point of departure, several panelists cited the value of redundancy to help reduce consequences.

In addition, it was observed that it is inappropriate to deal with security issues after the fact. Thus, it was critical to start mitigation early, beginning with the development phase of new technologies. For all organizations, mission must come first (e.g., IRS collects taxes), and they will use new technologies to aid that mission. With this in mind, security has to be part of the innovation and development of new technologies.

One of the panelists defined risk as the product of three terms: threats, consequences, and vulnerabilities. Note that cyber risk accumulates. For example, risk (annualized expected loss) from cyber is being allowed to build up without being charged as a cost, because most of it hasn’t had to be paid out yet. Key issues associated with risk depend heavily on resiliency and restoration time. In his presentation, the panelist highlighted two critical infrastructure industries for which the Gross Domestic Product (GDP) was most dependent (i.e., 72% dependent on electric power and 71% dependent on oil and gas fuel).

The panelist also proposed three recommendations for the new Administration. First, it is important to develop a National Cyber Recovery Plan for large scale attacks on critical infrastructure industries. One way to mitigate this risk is to diversify friendly targets. Second, there is a need to create a National Cyber Policy Board to review and direct national cyber-security measures. It is anticipated that this Policy Board would work closely with a Deputy National Security Advisor for cybersecurity. Finally, there is the need to establish a Cyber Security Rating Agency to evaluate the security of commercial-off-the-shelf (COTS) software. The activities of this agency might be analogous to organizations that perform automobile crash ratings or energy efficiency ratings.

For immediate improvement of our operational preparation and responsiveness, one of the panelists recommended strongly that we create a government funded National Crisis Coordination Center. This center would house government, industry, and academic security experts, both in the physical and cyber domains. Among its functions it would jointly prepare, exercise, evaluate, and update National Joint Crisis Response plans to prevent, detect, and respond to incursions. In addition, it would conduct joint exercises at the national level to train and test the plans.

In addition, several of the other panelists urged the community to implement best practices (e.g., policy enforcement; e-mail security, fight SPAM). As an example, it would be useful to encourage people to register outbound mail IP addresses. This could reduce the amount of spam by 50% and one could immediately be able to tell if the sender is registered.

Furthermore, one of the panelists observed that there is a greater risk from data manipulation, as opposed to data denial. This is an issue that requires additional attention.

#### E. Theme: Partnerships

The third major theme of the conference addressed the issue of partnerships. Initial public-private partnerships have generally been disappointing, with few exceptions (e.g., Infragard). However, it was stressed that Government can **not** do it alone. It is imperative that the private sector cooperate. To implement that concept, the private sector must be fully integrated at **all** stages of security efforts. In addition, cyber experts must inform industry about steps to reduce risk. However, several of the panelists articulated a concern: If we are not careful, Government laws and regulations can impede progress. To deal with this concern, several panelists noted that perhaps we need to implement the concept of “megacommunities”, bringing together public, private, and civil sectors. This concept is articulated in the book by that name that was recently issued by senior members of Booz-Allen-Hamilton.

#### F. Theme: Information Sharing

The fourth major theme of the conference dealt with the issue of information sharing. Currently, very limited effective sharing is performed between public-private participants. One opportunity to enhance that sharing is to adopt key standards. One of the panelists noted that it would be equivalent to adopting the standards of a certified public accountant. More specifically, one of the panelists recommended that we provide an authoritative structure for codifying, evolving, and using informed expert judgment to apply known standards, practices, and other criteria for cybersecurity (e.g., developing criteria to identify varying levels of security).

However, there are a number of challenges that need to be overcome if there is to be effective sharing between public and private participants. First, there is a need to address over-classification that currently limits sharing (e.g., the tension between classification versus disclosure). Second, there is an inherent tension between the equities of the Government (which is charged with protecting confidentiality) and industry (which is trying to minimize time to market). One panelist noted, however, that due to the risk of loss of intellectual property, a shift to confidentiality is under way in the private sector.

Historically, we have seen the Government change policies and invest in different areas and technologies. Conversely, industry is driven by new technologies, new priorities, new policies, and new laws. In addition, one of the panelists recommended that we make better use of tools and organizations in place. As an example, he recommended that we fully integrate private sector, state, local, tribal, and key international into planning, operations, and exercise at every phase as full and equal partners.

#### G. Theme: Education and Training

The fifth major theme of the conference dealt with the issue of education and training (E&T). There was general agreement among the panelists that cyber E&T is limited, at all levels. In particular, there is a

need to educate key elements to address cyber decisions from a risk management perspective. This includes E&T of policy makers, users, and affected organizations. One of the panelists cautioned that we must educate policy makers, but cyber experts should deal with the specific details.

One of the most effective ways of implementing E&T is to perform **Interagency** exercises. However, several panelists observed that those activities are not sufficient unless we develop and implement meaningful “lessons learned” (vice “lessons recorded”) from that process.

Another panelist noted that education for developers and code writers is deficient. Many do not have the proper training to be able to write secure code, and as a result, the commercial products they put out are more susceptible to manipulation.

#### H. Theme: Cybercrime

The sixth major theme of the conference dealt with the issue of cybercrime. Several of the speakers and panelists emphasized that the threat is real (and expanding)! The speakers said that “We are losing the global cyber war at an accelerated rate!” In addition, they stated that “Cybercrime is effective because you can try to commit crimes an infinite number of times; you need to succeed only a few times!” Overall, it was stated that there are three elements of the threat: crime; industrial espionage; traditional espionage. It was further noted that criminal attack vectors are comparable to those of state attacks.<sup>1</sup>

The speakers recommended that we focus on the “top 25 Common Weaknesses Enumeration (CWEs)”, and many of the panelists observed that current laws to deal with these issues provide limited value. As noted above, a major weakness is the inability of Web developers and code writers to write secure code, increasing the risk of cybercrime.

This raised the following question: When will the tide turn? It was suggested that we will make useful headway when we implement the following steps. First, it is critical to create safer software. One recommendation was to make business partnerships contractual (e.g., require the company to fix future flaws and security problems in the software). Second, it was observed that we need to stop existing attacks (e.g., actions by the Department of Justice and computer security specialists). However, in order to do so, we need to find the needed talent. As an aside, it was observed that China’s People Liberation Army (PLA) periodically runs national talent searches for the best hackers.

Overall, there was unanimity: We need to take decisive actions immediately!

---

<sup>1</sup> As an example, the top eight most dangerous attack vectors were identified as: web site attacks to plant browser exploits; targeting phishing attacks/spear phishing; malware in embedded devices; browser scripting attacks that turn a browser into a communication channel; the latest Metasploit releases; pass-the-hash tools widely available; fast-flux bot-nets; and cold boot attacks (source: [www.sans.org/tools.php](http://www.sans.org/tools.php))

## I. Theme: Cyber R&D

The seventh major theme of the conference dealt with the issue of cyber R&D. The panelists concurred that the problem is inherently Interagency. To fight for R&D dollars, we need to make people aware how cyber underlies many different sectors. As a result, we need to develop a federal R&D strategy that is inherently Interagency. Consequently, we need to improve efforts to plan and implement R&D, collaboratively.

The government holds a powerful position in that it can quickly change the R&D status quo by changing policy and by investing in various technologies and related fields. Since industry is driven by new technologies, policies and laws, it is largely subject to government action. For this reason, the panelists urged the government to take a more activist role in driving R&D. This ties back to the theme of leadership mentioned above.

The panelists also emphasized that cyber security can not be treated as an after-thought. It must be an integral part of the innovation and infrastructure/product development that will characterize the cyber architecture of the future.

Among the key challenges affecting the cyber community is the issue of attribution. Our R&D efforts must lead to innovative ways to address this issue if we are to effectively deal with the myriad challenges of cyber defense, exploitation, and attack.

## J. Theme: International Dimension

The eighth major theme of the conference dealt with the issue of the international dimension of the cyber problem. The cyber problem is inherently international and must be treated as such. For example, attacks against friends and allies are usually routed through multiple countries. Consequently, we need more international laws, training, and operational standards. These include tactics, techniques, and procedures to physically pursue aggressors as well as necessary legal actions to support prosecuting an aggressor. Thus, there is a need to deal with the legal, governance and treaty issues from this perspective.

As with all attempts at achieving an international consensus on policy agreements, each country will have different strategic priorities with regard to cyber governance and laws. One of the panelists recommended that we make US representation to relevant international standards bodies more robust.

## K. Theme: Next Steps

The final major theme of the conference addressed next steps. There was near-unanimity that the new Obama Administration should NOT “start over” or engage in a lengthy study while postponing action. An excellent foundation exists with the innovative ideas associated with CNCI and the recently-released CSIS cyber study. However, it would be useful to conduct a review of those initiatives to clarify risks and to prioritize follow-on actions. Shortly after the NDU conference, it was observed that a 60 day review was to be conducted of on-going efforts to establish a firm foundation for future cyber actions.

## L. Summary

The conference brought together an interesting cross-section of the stakeholders that comprise the cyber community (e.g., US Government Agencies, industry, academics, not-for-profits). As an organizing principle, the conference was organized into a set of key panels to address five key issues: Cyber Attacks, Preparedness, and Responses; Cyber Risk; Malicious Activity and Cybercrime; R&D Requirements and Planning; and Governance of Cyber: Strategic Priorities.

However, from the presentations and discussions, nine key themes emerged: Leadership and trust; Risk management; Partnerships; Information sharing; Education and training; Cybercrime; Cyber R&D; International dimension of the problem; and Next steps. In addition, many of the panelists put forth key recommendations for the new Administration. A selected set of those recommendations is summarized in Appendix B.

Follow-on conferences and workshops will be convened to assess these themes more deeply. In particular, the next CTNSP-sponsored conference will focus on the international dimension of the problem.

## Appendix A.

### CNCI Initiatives:

The following material is excerpted from the article “Details Emerge about President’s Cyber Plan” (November 21, 2008).

**1. Move towards managing a single federal enterprise network.** The cornerstone to this effort is the Trusted Internet Connections program, initiated by the Office of Management and Budget in November 2007 that aims to reduce the number of connections from federal agencies to external computer networks to 100 or fewer, from more than 4,300 connections identified in January of this year. But it would also rely heavily on **Federal Desktop Core Configuration** standards, initiated by OMB, which prescribe specific requirements to access and use federal networks. –

**2. Deploy intrinsic detection systems.** These systems would build on current software tools—notably a program called Einstein, and an enhanced version called Einstein 2, developed by the Department of Homeland Security. These tools monitor and identify information streams at network access points, but currently lack the ability to do more than report potential problems.

**3. Develop and deploy intrusion prevention tools.** DHS teams are now working on the development of Einstein 3, which would be designed to block and mitigate malicious patterns in the code surrounding information in transit, before they can do harm on federal networks. -

**4. Review and potentially redirect research and funding.** Efforts are underway to take stock of cyber research and related programs and to look for overlaps and gaps, in order to channel resources more effectively.

**5. Connect current government cyber operation centers.** In particular, increase the effectiveness these centers by standardizing operating procedures and improving shared awareness of threats.

**6. Develop a government-wide cyber intelligence plan.** Because several civilian, intelligence and defense agencies have varying responsibilities to address cyber threats, the government has had a difficult time crafting a single, coherent approach.

**7. Increase the security of classified networks.** The escalating volume of attacks and the increasing penetration into supposedly secure networks makes it imperative that work be done to further secure classified networks and the information on them.

**8. Expand cyber education.** There is a significant need for creating a career pipeline to train cyber security experts—with offensive as well as defensive skills—and to institutionalize the knowledge surrounding security threats. Cyber education needs to include developing a broader base of candidates with scientific knowledge and a cyber-savvy workforce, as well as network specialists who can work in law enforcement, military, homeland security, health and other specialty areas.

**9. Define enduring leap-ahead technologies.** The government needs to provide direction for “game-changing” technologies that would provide a more stable environment and supplant some of the fundamental design of existing technologies--and the current patchwork approach to fixing them.

**10. Define enduring deterrent technologies and programs.** The government has an opportunity to tap broader groups of scientists, strategists and policy makers – similar to the way it did a half-century ago in crafting a nuclear weapons deterrent strategy—to develop new and lasting approaches to address cyber threats in this century.

**11. Develop multi-pronged approaches to supply chain risk management.** The reality of global supply chains presents significant challenges in thwarting counterfeit--or maliciously designed—hardware and software products which must be addressed.

**12. Define the role of cyber security in private sector domains.** Experts agree the government must do more to get its cyber security house in order. But with so much of the nation’s infrastructure in the hands of the private sector, more must be done to quantify the financial and economic risks associated with cyber security threats in order to provide better investment.

Major recommendations of the CSIS study, “Securing Cyberspace for the 44<sup>th</sup> Presidency”:

- Create a Comprehensive National Security Strategy for Cyberspace
- Organize for Cybersecurity (e.g., appoint an assistant for cyberspace; establish a Cybersecurity Directorate in the NSC; create a new National Office for Cyberspace (NOC); create three new public-private advisory groups to support the assistant for cyberspace and the NOC)
- Partner with the Private Sector (e.g., create a new presidential advisory committee that would incorporate the National Security and Telecommunications Advisory Committee (NSTAC), National Infrastructure Advisory Council (NIAC))
- Regulate for Cybersecurity (e.g., task the NOC to develop standards and guidance)
- Secure Industrial Control Systems and SCADA (e.g., the NOC should work with regulatory agencies and the National Institute of Standards and Technology (NIST) to develop regulations for industrial control systems)
- Use Acquisition Rules to Improve Security (e.g., the US Government should work with industry to develop and implement security guidelines for the procurement of IT products; take steps to increase the use of secure Internet protocols)
- Manage identities (e.g., make strong authentication of identity a mandatory requirement for critical cyber infrastructures)
- Modernize Authorities (e.g., have the Department of Justice reexamine the statues governing criminal investigations of on-line crime)
- Revise the Federal Information Security Management Act (e.g., use performance-based measurements of security)
- End the Division between Civilian and National Security Systems (e.g., adopt a risk-based approach to federal computer security)
- Conduct Training for Cyber Education and Workforce Development (e.g., create training programs and career paths for the federal cyber workforce)
- Conduct Research and Development (R&D) for Cybersecurity (e.g., provide overall coordination of cybersecurity R&D; increase investment in longer-term R&D cybersecurity)

## Appendix B. Selected Speaker Recommendations:

During the course of the conference, a number of recommendations were proposed for the Obama Administration. A selected set of those recommendations is summarized below.

- Develop a National Cyber Recovery Plan for large scale attacks on critical infrastructure industries. Mitigate the risk by diversifying friendly targets.
- Create a National Cyber Policy Board to review and direct national cyber-security measures. This Policy Board would work closely with a Deputy National Security Advisor for cybersecurity.
- Establish a Cyber Security Rating Agency to evaluate the security of commercial-off-the-shelf (COTS) software.
- Provide an authoritative structure for codifying, evolving, and using informed expert judgment to apply known standards, practices, and other criteria for cybersecurity (e.g., develop rating criteria to identify varying levels of security).
- Create a government funded National Crisis Coordination Center to jointly prepare, exercise, evaluate, and update National Joint Crisis Response plans to prevent, detect, and respond to incursions. It would also conduct joint (interagency) training exercises at the national level to test the plans.
- Manage identities (e.g., make strong authentication of identity a mandatory requirement for critical cyber infrastructures)
- Start a drive to register outbound mail IP addresses. This could reduce the amount of spam by 50% and one could immediately see if the sender is registered.
- Increase educational requirements for web developers and code writers, many of whom do not know how to write secure code.
- Create network compartmentalization; assess the value of assets and where risks are and compartmentalize accordingly.
- Make cyber security a major part of technological innovation and development. Infrastructure and product designs must be developed with cyber security in mind.
- Find a creative way to identify and recruit the best talent the US has to offer. Foreign rivals are outpacing the US with respect to personnel.
- Focus on reducing consequences instead of vulnerabilities. Vulnerabilities are hard, or impossible, to eliminate. Redundancies reduce consequences.
- Develop a federal cyber R&D strategy, including the following

- Develop application layer dependent security solutions;
  - Develop and apply risk analysis tools for supporting investigations in cyber security;
  - Develop and apply agent-based simulation models for forecasting results of policy/legislative cyber security solutions.
- Increase US representation to relevant international standards bodies in order to press for more international laws, training, and operational standards.

## Appendix C. World Information Technology and Services Alliance (WITSA) Resolution on Cyber Security

At the WITSA meeting in Hyderabad, India, on December 2, 2008, the following cyber security principles were formulated:

- The Internet and information networks are global in nature; therefore, cyber security requires international collaboration through bilateral and plurilateral efforts and through multilateral organizations that enables flexibility, innovation, and private sector leadership;
- Information networks are ubiquitous and used by so many for their communications needs and operations; therefore, governments and organizations should address cyber security as a fundamental and cross-cutting issue;
- Industry and government share an interest in the proliferation of a free and open Internet, electronic commerce, other value-added networks, and an efficient, effective information infrastructure; therefore, cyber security efforts should be undertaken in a way that does not inhibit innovation;
- There is no static or one-size fits all solution to “perfect” cyber security; therefore, cyber security efforts should be part of a dynamic, risk management-based approach to protection, detection, and mitigation;
- No on entity can solve cyber security issues alone; therefore, government and industry must find ways to collaborate, share information and analysis, and identify appropriate roles and responsibilities for protection, detection, and mitigation efforts both domestically and internationally, including adapting existing laws, if necessary;
- Our global networks provide critical communications and operational services to government, industry, and individuals around the world; therefore, in order to further assure those services, cyber security should be considered as a fundamental and foundational tenet in all efforts such as the development of government services, company product design, and consumer behavior;
- Companies and individuals have been increasingly targeted by cyber criminals from all over the world; therefore, law enforcement agencies must have the ability to collaborate and cooperate on a global basis, and criminal statutes must incorporate cyber crime so that those criminals can be prosecuted.