



Date: 3 September 2008

Location: SAIC Conference Center, 1710 SAIC Drive, McLean, VA 22102

Summary Report

On Wednesday, September 3, 2008, a distinguished group of senior leaders and experts from across the federal government, the private sector, and academia convened at the SAIC Conference Facility in McLean, Virginia to participate in a Thought Leadership Symposium entitled, "Cyber Challenges for the 21st Century." The symposium featured prepared remarks by nationally recognized leaders representing the Department of Defense, the Office of the Director of National Intelligence, the National Security Agency, and the private sector. Symposium participants interactively contributed their perspectives on the current state of cyber and on the challenges facing the government and the private sector as the nation advances further into the 21st century.

The event was one of a series of SAIC-sponsored symposia and conferences designed to stimulate discussion on and bring focus to significant national security challenges. The conceptual framework for this symposium was built around the premise that the very fabric of our social, economic, political and military power is dependent upon our ability to develop and maintain a secure cyber infrastructure. Achieving success in this endeavor will require building effective partnerships among the Department of Defense, the Department of Homeland Security, the Intelligence Community, other interagency players, and the private sector.

As background for the symposium, participants were reminded that, as Americans have progressed into the 21st century, our information infrastructure has rapidly become a key center of gravity, supporting fundamental elements of our daily life. Because of its intrinsic importance in American society, cyber criminals, cyber terrorists, violent non-state actors, and even nation-states view the cyber domain as the battlefield of choice for asymmetric attacks on America, threatening the security of and confident access to America's cyberspace infrastructure.

The primary task given to the participants was to interactively examine, and propose possible solutions to, cyber challenges facing the nation in an effort to help "move the ball forward" on this challenging set of national security issues. The agenda (attached) focused on assessing four key areas that are impacted in the race to secure cyberspace: (1) Human Capital; (2) Cyber Deterrence; (3) Personal Privacy; and (4) the Role of Government and Private Sector Cyber Collaboration.

The remainder of this summary will highlight the key points and takeaways from each of the four primary sessions, providing main issues from both the initial principal speakers who introduced the topic and dialogue, the related panel discussions, and the question and answer period following each session.

Human Capital

Overall Needs. The pervasiveness of cyber human capital needs in the government and private sectors was one of the primary issues addressed. Several key points highlighted this issue and included: cyber is an intrinsic segment of everything we do and therefore issues surrounding cyber human capital are an “entire workforce” problem; we need to train and retain a group of people who understand all aspects of cyber, e.g., laws, policies, offense/defense and the rapidly changing aspects of the cyber domain; and, we also need to better leverage what capabilities we already have in organizations like DISA, DNI and the Services.

Recruitment. Symposium attendees recognized that the lack of a qualified workforce in cyber was a key human resource challenge necessitating further attention. It was stressed and noted among several attendees that the cyber human capital deficit in the United States currently cannot be met by universities because they are not graduating enough students in the issue area.

The Department of Defense, specifically, is finding it challenging to fill an ever-increasing demand for individuals with specialized skills in the subject matter. Participants discussed the need to develop clear career paths for members of all of the Services engaging in cyber. Additionally, symposium attendees noted that it would be important to elevate the cyber field to a rated profession at the war-fighting level for military personnel. Discussion also touched on an Air Force initiative that sends high-aptitude cyber specialists to Officer Candidate School for promotion to the officer rank.

Panelists posited avenues that could be further explored may include the utilization of existing government partnerships with universities, the creation of scholarships, and the use of recruitment with strong monetary and educational incentives to attract individuals into the government cyber arena as opposed to having them enter into private industry. It was further noted that recruiting Departments and Agencies must stress to candidates the uniqueness of opportunity and importance of the government arm in the creation of policy – an area in which the private sector cannot and does not participate – and these same Departments and Agencies must ensure that employees are recruited appropriately to develop policy. It was proposed that the government consider recruiting an industry “name brand” player to publicize the benefits of government service in cyber with the goal of attracting qualified people to government service.

While a majority government force was seen as ideal, participants acknowledged the need to ensure that a contractor force is integrated into the government cyber industry. As such, government civilian and contractor personnel require an active dialogue on how to integrate their efforts in the cyber field. Because of the nature of cyber, distinction between government and contractor will need to be transcended to a certain point to allow all of the operators – both government and contractor – to work together to understand the network and attain a common operational picture (COP).

Workforce Integration. Some participants discussed individual Service actions to create cyber awareness among the Services. For example, individuals familiar with the Air Force discussed actions to change the mindset of the members of the Air Force such that they would begin to view the Air Force Global Information Grid (AF-GIG) as an integral part of the weapons system. Participants familiar with the Navy reinforced these points with an active discussion addressing “How does the specialized cyber workforce interact with other parts of the Navy?”

Retention. Significant discussion focused on the issue of retention. Symposium participants discussed the Air Force “Total Force Initiative” as it has been manifested in the cyber community. Through the initiative, the cyber skills of members of the Air National Guard and the Air Reserve are being integrated into Air Force daily operations. Several panelists posed the idea that the military should consider offering a type of “continuum of service” option in which service members could move from military service to the reserves to private industry and back without great bureaucratic difficulty. It was also suggested that the government research the creation of a “ready-reserve” pool of private sector individuals skilled in cyber who could provide surge capacity in the case of an emergency or crisis. It was noted that these individuals would need to be paid for their willingness to be placed on retainer.

Leadership. The tremendous growth in the cyber industry led symposium attendees to agree that finding qualified individuals to serve as leaders in the issue area was difficult. Because much of the workforce is comprised of young recent university graduates, these individuals do not yet have the ability to fill GS 14/15 positions in the field. Individuals with the appropriate experience to provide the leadership needed are older, and because they did not enter adulthood with the technology of today, they are unable to “speak the language” of the technology or fully appreciate its impact on security and policy. Several possible remedies were offered for this situation, among them was a suggestion to create a mentoring program whereby “digital natives” (or those younger individuals who had grown up with the technologies) reverse mentor “digital immigrants” (or those individuals who are not intimately familiar with the technology).

Further Generational Issues. Many participants expressed concern over the perceived gap in the definitions (such as that of cyber privacy) between the newer generations, the “cybernatives”. It was agreed among participants that America’s cyber force requires rules of engagement. The dialogue surrounding these rules should encompass such issues as providing training on expectations of behavior and the manner in which people should operate. The dialogue should focus special attention on workforce-wide issues. Participants noted that, in addition to cyber professionals taking part in this dialogue, it was necessary to include other qualified professionals who have a solid understanding of the legal, civil rights, and civil liberties issues surrounding the rules of engagement.

Training and Education. Given the rapid pace of technological advance (as pointed out by Moore’s Law), a large part of the difficulty in maintaining a fully functional cyber force surrounds the need for constant training and retraining of individuals in the cyber field. Participants agreed that the rapid turnover in

technological knowledge requires the government and Services to develop retraining plans to a level that has never before been necessary. For the Department of Defense and the Military Services, this implies sending individuals to school several times a year instead of once every few years, as it has been the model in the traditional career fields. Participants familiar with the Navy noted that their cyber school curriculum has been outsourced to a contractor, in order to ensure it is constantly kept up-to-date in a manner that could not be guaranteed within the Navy's training structure.

Cyber Deterrence

Issue Overview. Symposium participants recognized the unique difficulties surrounding the concept of cyber deterrence. Traditional thinking on cyber deterrence often views it as a single element that stands alone, yet in fact, participants noted that cyber is but one element in the toolbox of overall 21st century deterrence. Participants generally agreed three threat levels face cyber: (1) Hacker/Individual level; (2) Industrial level; and (3) Nation-state level. Within the cyber arena, the identification of enemies is extremely difficult, and, when the enemy is determined, the question becomes "how", "why", and "where" to fight and "how do we gain the justifications, titles, and authorities needed to battle." There was extensive agreement on the fact that the internet, in warfare terms, is a disruption; however, it was noted that the disruption caused by the internet can be advantageous in modern warfare. Because of this, in matters of cyber deterrence, we must learn to operate in depth, be pervasive and think globally.

Deterrence Challenges. Participants agreed that the following questions pose serious challenges to the area of cyber deterrence: (1) What can we make concrete? (2) What should we leave to discovery? (3) What is too expensive for us to see? and (4) What are we not able to do at all? These questions, in turn, pose challenges to our operations in the cyber arena. Specifically, participants noted that all things cyber can be – at any point – turned on or off, reconfigured, and disguised. Additionally, the lack of clearly defined geographical boundaries and borders in the cyber arena further clouds the key issue of attribution of cyber activities. Participants also agreed that there exists great confusion on the issue of who is supporting, and who is being supported in the deterrence aspect of cyberspace. Transitions in the arena are occurring too quickly for the lead and supporting roles to be consistently clear between government and private sector players. Another key challenge posited was that our deterrence framework needs to avoid being "reactive only" - and that the best deterrent advantage occurs when adversaries realize that your networks can withstand whatever attacks that might be mounted.

Deterrence: Defense Only? The participants discussed the questions of whether a cyber defense-only strategy could be successful, and where does one draw the line between offense and defense in cyber operations? It was posited that a defense-only strategy may not prove successful, and that, in fact, offensive operations may be appropriate to guarantee the United States the ability to maintain the right to self-defense. Participants postulated that a broader issue in this debate is the question of how to build an operation in such a way that we understand the collateral damage that this operation poses across the broad

range of the network that may be touched by the operation. Some participants stated that it was important to have an effective way to model these effects, in order to accurately gauge the effects of an operation before it is conducted.

Cyber Declaratory Policy as Deterrence. It was noted by attendees that the United States lacks a cyber declaratory policy. Some participants wondered what type of role such a policy would play in deterring potential adversaries. It was discussed that a declaratory policy is just that – declaratory – unless there are teeth (real capabilities, doctrine, policy, and law) behind it that can provide confidence and credibility. The questions surrounding the issue then become: how would one put in place a declaratory policy without backing it up with “teeth”? Further, what would be the threshold at which the United States would take action? And, finally, at what point are we willing to put our credibility on the line and follow through? It was noted that, though there is definitely a place for a declaratory policy, without underpinning it with a concrete foundation, it loses its effectiveness, and can actually decrease security.

Cooperation in Cyber Deterrence. Currently, inside the United States, it is the responsibility of the Department of Homeland Security, supported by the Department of Defense, to defend the nation’s networks. Outside of the United States, the Department of Defense is the lead department working to protect the United States from cyber attack. The aforementioned arrangement fits within the existing body of law. It was the opinion of the participants that this arrangement would continue until it was proven by an event to be disadvantageous for protecting the nation’s networks. Participants discussed the fact that, after that point, the nation would need to make a decision, as needed, to change laws, and thereby change the construct.

Some participants questioned whether our allies share our dependence, concern, and interest in cyberspace security. It was stated that, our allies absolutely share this concern. Participants noted that, in reality, nothing that occurs in cyberspace happens without someone else noticing. The parties noticing may not understand the rationale and effects of the action, but these parties can see movement and infer information from that. Some participants argued that, in order to be effective in cyber, the United States was going to have to cooperate with its allies to develop international law – an effort that has not been historically successful in other parallel situations. It was surmised that this law change would first have to manifest in bilateral agreements between nations, and then, when nations begin to realize the limitations of bilateral agreements, relations would move beyond the bilateral arena into multilateral pacts. Some participants mentioned the Law of the Sea as a model for this type of action.

A spirited discussion centered on the question of civil/military cooperation in cyberspace. For instance, the private sector, law enforcement, and the Departments of Defense and Homeland Security each address differing levels of threats facing cyber, but it is uncertain how they work together to deter threats. Establishing clear roles and responsibilities and rules of engagement will help define a cyber doctrine, law, and policy, and in turn support a deterrence strategy. These challenge areas are gaining national prominence and are only beginning to unfold to the nation. It was suggested and generally agreed that the

issues impacting a cyber deterrent strategy will become part of a larger cyber debate that will take center stage in the next Administration.

Personal Privacy

FISA. The Foreign Intelligence Surveillance Act of 1978 (FISA) was enacted by Congress and prescribes procedures for physical and electronic surveillance as well as for the collection of “foreign intelligence information” of individuals, including American citizens and permanent residents suspected of being engaged in espionage and violating U.S. law on territory under the United States’ control. It was pointed out that personal privacy is a constitutional issue and that monitoring has been viewed as a “personal search.” Additionally, U.S. citizens have a “reasonable expectation” of privacy within the cyber domain. Through FISA, Congress has attempted to regulate the capability of the government to meet the “reasonableness” requirement.

Recent FISA amendments have updated the legislation to respond to changes in technology and security challenges. Four primary personal privacy issues were addressed in the recent Congressionally-approved (2008) modifications to the original FISA legislation. These were: collection of data (what personal privacy rights are impacted by collection means?); retention of collected data (how long is the data retained and who has access?); information sharing (with whom can the USG share collected data?) and what requirements exist for audits, oversight and reporting of FISA-related activities? It was noted that NSA was required to demonstrate how it addresses all four of these issues during recent FISA testimony.

Participants in the symposium had a rousing discussion of the actual effectiveness of these actions. Many attendees agreed that the boundaries between various activities are more ambiguous in these areas than the law implies. In addition, attendees found that the issue is not one of collection; it is that individuals involved in collection are unaware that their data has been collected and the security of that data has been compromised. There was general conversation that it would be necessary for the American populace to involve itself in the search for “balance” between the need for information surety and the need to share data through a national dialogue or debate.

Data Collection. It was generally agreed among participants that several issues surrounding the collection of data associated with cyber activity are not yet completely resolved, despite the four personal privacy issues addressed by the FISA Modification Legislation noted above. Additional issues raised included: How do you protect U.S. citizens’ information? How do you handle the data when it is relevant? What do you do with data if it proves not to be relevant? The attendees also agreed that the need for auditing and oversight of these issues lends itself to a public policy issue and that policy makers need to socialize ideas about what can be done to ensure cyber defense while still protecting civil liberties. Policymakers will also have to provide rules of engagement and plans of action to build confidence into the system when mistakes occur.

Personal Privacy and the Military Services. The point was made by some participants that the United States Military is the most trusted institution in America. If any issue arises with regard to the Armed Services and personal privacy, this issue will irrevocably damage the reputation and harm the credibility of the Services. For this reason, among others, the Armed Services need to be aware and vigilant against this type of personal privacy loss – in the same way that the government and private industry should be.

Government and Private Sector Collaboration

The Government and the Threat. Attendees participated in a vigorous discussion surrounding the threat faced by the government in cyberspace. Related to this discussion are several questions on how to optimize the capabilities of the government to respond to the threat. Among those questions: How do we utilize intelligence communications to inform the debate? How do we optimize the capabilities of the DoD to respond to the threat? How do we coordinate a unity of effort across the government? Participants discussed the fact that the current cyber security approach of the government is ineffective. The system is overwhelmed, and this results in inconsistent threat detection and an inconsistent response to threat. Most participants agreed that, if the United States does not change its current path, the nation will face significant losses to current and future cyber threats.

Distinctions between .mil/.gov and .com. There was a rousing discussion among the participants about making distinctions between the need for security in .mil/.gov domains before .com. Participants were not in agreement over the correct manner in which to make these distinctions. Some stated that the cyber enemy is indistinguishable, and thus the nation can't make arbitrary decisions to only focus on the .mil and the .gov domains. Others argued that the government needs to "get it right" in a smaller domain space before it can translate its accomplishments into the world of .com.

Private Industry Incentive to Partner with Government. Participants discussed the motivation behind a business model for security developed by private industry for the government. Issues arose over the question of how private industry can effectively sell the proposed model to its shareholders. Industry participants commented that turnover amongst government personnel involved in development of procedures and standards posed a problem. Attendees theorized that, if there was policy at a high level driving the cyber security decisions, corporations and their shareholders might have more interest in developing improved security solutions for the government. It was also noted that the creation of general standards guidelines would also be useful in this process.

Other Issues

The Change in Administration. With the upcoming Presidential elections in November, the United States government will undergo a change in administration. With this change, large amounts of personnel turnover occur in the highest levels of the government. Participants generally agreed that there needed to be a discussion of the cyber issue at these levels and in the Congress of the United States. Participants also widely agreed that these issues should not be brought to the attention of the individuals now; these discussions will need to wait until the new administration has completed transition. Some attendees questioned whether it was prudent to wait, and most responded with the fact that, whether prudent or not, there was no choice but to do so. Attendees alluded to the fact that members of both of the political campaigns' advisory staffs had been alerted of the issues surrounding this subject, and that both hopefully have a sense of the gravity of the issues. All attendees agreed that, once the new administration is in place, it is imperative that there be a national debate on the issue of cyber.

Attribution. Participants mentioned attribution several times throughout the Symposium. All participants seemed to agree that the need for an attribution capability was strong, but that the question of determining attribution was a very difficult one. Determining a solution to the attribution question, however, would be very useful in knowing who to watch and when to turn on the right types of filters to deter those individuals being watched.

The Future. The future of cyber is upon us and attacks in the cyber domain occur every day. The most significant cyber issues need to be highlighted and discussed at the national level. Unfortunately, however, it sometimes takes a catastrophic event to drive action. It remains to be seen whether this will be the case in cyber.



CYBER CHALLENGES FOR THE 21ST CENTURY

Date: 3 September 2008

Location:

SAIC Conference Center, 1710 SAIC Drive, McLean, VA 22102

Agenda

7:45 – 8:15 AM..... Attendees Arrive/Check-In
Coffee, Juices, Fruit and Pastries in Conference Center

8:15 – 8:30 AM..... Administrative & Opening Remarks
Administrative Remarks
Mr. Tom Neary, Vice President and Director, Thought Leadership Strategies,
SAIC

Welcome/Opening Remarks
Ms. Deb Alderson, President, Defense Solutions Group, SAIC

8:30 – 8:50 AM..... General James Cartwright
General James Cartwright, Vice Chairman, Joint Chiefs of Staff, will provide the
Symposium Keynote Address, speaking on the concept and national policy
implications of Cyber Deterrence.

8:50 – 9:00 AM..... Q & A with General Cartwright

9:00 – 9:45 AM.....Panel Discussion
Mr. Rich Haver, Vice-President for Intelligence Programs, Northrop Grumman
Corporation, will chair a panel of distinguished experts who will address a spectrum
of issues associated with Cyber Deterrence.

9:45 – 10:05 AM.....Ms. Priscilla Guthrie
Ms. Priscilla Guthrie, Director, Information Technology and Systems Division,
Institute for Defense Analyses and former Deputy Chief Information Officer for the
Department of Defense, will address critical challenges and issues surrounding
Cyber Human Capital and the need for a high quality, highly trained and educated
Cyber Operations and Security Cadre for America.

10:05 – 10:15 AM.....Q & A with Ms. Guthrie

10:15 – 11:00 AM.....Panel Discussion
RADM Michael Brown, Deputy Assistant Secretary for Cyber Security and
Communications in the National Protection and Programs Directorate, Department
of Homeland Security, will chair a panel of distinguished experts who will analyze
the issues surrounding the need for high-caliber Human Capital in America's Cyber
Domain.

11:00 – 11:15 AM..... Break

11:15 – 11:35 AM.....Mr. Vito Potenza

Mr. Vito Potenza, General Counsel, National Security Agency, will speak on “The Impacts of Personal Privacy Issues on Cyber Operations”

11:35 – 11:45 AM.....Q & A with Mr. Potenza

11:45 – 12:30 PM.....Panel Discussion

Dr. Charles Palmer, Director of Research and Chair of the Institute for Information Infrastructure Protection and Chief Technical Officer for Security and Privacy, IBM Research, will chair a panel of distinguished experts who will further assess the impacts of Personal Privacy Issues on Cyber Operations in America.

12:30 – 1:30 PM.....Lunch

Catered Lunch.....attendees are invited to dine in the Symposium conference room.

1:30 – 1:50 PM.....Ms. Melissa Hathaway

Ms. Melissa Hathaway, Senior Adviser to the Director of National Intelligence and Cyber Coordination Executive, will address Government and Private Sector Partnerships in securing America’s Cyberspace and enhancing our global competitiveness.

1:50 – 2:00 PM.....Q & A with Ms. Hathaway

2:00 – 2:20 PM..... Mr. Bill Vass

Mr. Bill Vass, President and Chief Operating Officer of Sun Microsystems Federal Corporation, will speak on the role of Government and Private Sector Collaboration in our nation’s Cyber Domain.

2:20 – 2:30 PM..... Q & A with Mr. Vass

2:30 – 3:15 PM.....Panel Discussion

Mr. Robert F. Lentz, Deputy Assistant Secretary of Defense for Information and Identity Assurance in the Office of the Assistant Secretary of Defense, Networks and Information Integration/Chief Information Officer, will chair a panel of distinguished experts who will further examine and address United States Government and Private Sector Collaboration issues raised by Mr. Vass and Ms. Hathaway.

3:15 – 3:30 PM..... Conference Wrap Up

3:30 – 4:00 PM..... Informal Discussions

The Symposium conference room will remain open until 4:00 PM for informal, post-conference discussions.