Booz | Allen | Hamilton

Cyber Strategic Inquiry

Enabling Change Through a Strategic Simulation and Megacommunity Concept

Cyber Strategic Inquiry 2008

Enabling Change Through a Strategic Simulation and Megacommunity Concept

EXECUTIVE SUMMARY

Cyber Strategic Inquiry 2008 (CSI'08) sponsored by Business Executives for National Security (BENS) and executed by Booz Allen Hamilton, brought together over 230 leaders from government, industry and society to generate a shared knowledge of cybersecurity risks and potential solutions. CSI'08 provided participants the opportunity to examine the emerging threats to our nation's competitiveness in this network-based age as well as potential opportunities to address these challenges through a strategic simulation. The infrastructure and digital devices that contribute to our global leadership on many fronts are now a key target for criminals, potential adversaries and malicious individuals. CSI'08 took place on 17 and 18 December, exposing participants to multiple, simultaneous situations and events that created confusion and doubt throughout society and demonstrated a widespread and serious impact on our nation's ability to function.

CSI'08 identified several key insights:

- The unique nature of cybersecurity requires clear lines of authority for planning and executing the cyber mission
- Enhanced and updated legal frameworks are required to support the full-spectrum of cybersecurity challenges, including the balancing of privacy with information sharing
- The complex, global and interconnected nature of the Internet may require an evolution in thinking about risk management and resilience
- The complexity of the cyber threat requires a codified and flexible response plan to effectively manage cybersecurity and facilitate public awareness and education
- Greater and more instantaneous cooperation among government, industry and society can enhance cybersecurity situational awareness
- Cybersecurity solutions can be enhanced by leveraging innovative technologies and the unique capabilities of government, industry, academia and the broader society

This After Action Report provides an overview of the approach and details on key insights developed during CSI'08. Following CSI'08, recommendations were developed based on a synthesis of these insights. Recommendations are not designed to be prescriptive, but seek to identify possible solutions to improve our nation's security and competitiveness through improved cybersecurity.

THE CHALLENGE

The United States is facing a serious economic and national security challenge:

Our government and private sector networks and information are being exploited at an unprecedented scale by a growing array of state and non-state actors. Malicious cyber activity continues to grow more sophisticated, targeted and serious; these trends will not just continue, but expand and increase in volume and complexity. Our nation must act quickly to protect critical infrastructures—on which our economy, government and national security rely—from exploitation, manipulation, disruption or destruction.

Our complex, interconnected networks create interdependencies that both increase vulnerabilities and increase the requirement for collaborative efforts to mitigate them. As such, cybersecurity is too large and complex for any one authority to handle alone. A new type of tri-sector leadership is needed, in which government, business and civil society work together in a common quest that benefits each sector without requiring them to give up their individual core identities or values.

To increase understanding of the cybersecurity vulnerabilities facing our nation and the potential remedies, the non-profit, non-partisan Business Executives for National Security (BENS) and the strategy and technology consulting firm Booz Allen Hamilton developed *Cyber Strategic Inquiry 2008 (CSI'08).*

PURPOSE

CSI'08 brought together more than 230 industry, government and institutional leaders to create a shared understanding of cybersecurity risks and potential solutions. Participants explored common vulnerabilities, identified public-private solutions–including effective information sharing partnerships–and generated a shared vision of the strategic investments required to seize future opportunities while addressing today's challenges.

CSI'08 Objectives

- Create awareness of the urgency for government, business and civil society to address the shared risks and opportunities inherent in cybersecurity
- Identify activities that will enable public and private sectors, and other elements of civil society, to work together to identify new solutions for assuring the resilience of our cyber infrastructure
- Generate a shared vision of the responsibilities and investment strategies (e.g., talent, technology, money, leadership) that will be required in government, business and civil society to meet future cybersecurity and resilience challenges
- Explore the attributes of persistent means–for example, a Cyber Megacommunity–that will enable affected public and private entities and other elements of civil society to more effectively and openly address cybersecurity challenges and opportunities

For the purposes of CSI '08, cybersecurity was defined as: *Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wired communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and non-repudiation.*[1]

---

1 "Non-repudiation" refers to programs which provide authentication of the origin and integrity of digitally transmitted data.

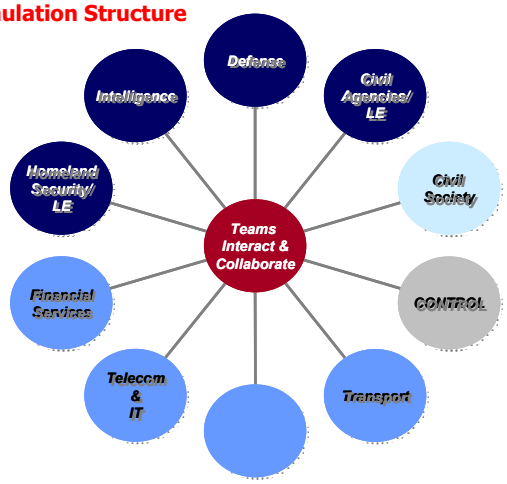
THE SIMULATION

CSI'08 included presentations by keynote speakers from government and industry, as well as a two-day simulation. Keynote speakers included:

- Cristóbal Conde, President and Chief Executive Officer, SunGard
- General James E. Cartwright, USMC, Vice Chairman of the Joint Chiefs of Staff
- Dan Hesse, Chief Executive Officer, Sprint Nextel
- Secretary Michael Chertoff, then Secretary of the Department of Homeland Security

The CSI'08 simulation was designed to represent a variety of functional/ stakeholder interests and highlight interconnectedness in a challenging scenario environment. Participants were organized into eleven teams comprised of nine Stakeholder Teams, an Assessment Team that provided feedback on the Stakeholder Teams' actions, and a Control Team that both oversaw simulation play and reacted for those elements not explicitly represented in the simulation. The

Exhibit 1
Simulation Structure



Stakeholder Teams included: government teams representing Defense, Civil Agencies/Law Enforcement, Intelligence, and Homeland Security/Law Enforcement; and industry teams representing Financial Services, Telecommunications and Information Technology, Energy, and Transportation; and a Civil Society Team.[2]

The simulation consisted of two moves, followed by an insights session. The Move 1 scenario focused on multiple, simultaneous cyber incidents affecting multiple sectors. The Move 2 scenario added in multiple, cross-sector cascading effects. In each move, teams identified how the incidents affected their sector and identified mechanisms to coordinate and collaborate. During the final insights session, teams identified critical steps that could be taken to develop a persistent engagement model for cybersecurity.[3]

INSIGHTS AND RECOMMENDATIONS

Leadership and Governance

The unique nature of cybersecurity requires clear lines of authority for planning and executing the cyber mission. Several teams perceived the lack of a credible, single leadership voice to address cyber policy issues and the time-sensitive responses needed to limit damage from or defend against cyber attacks. Participants noted that there needs to be a commonly understood cybersecurity vision and commonly accepted rules of engagement for government, industry and civil society. However, there is tension between the un-regulated, distributed nature of the Internet and the designation of a single entity to direct an effective, coordinated response. Though there was no agreement on a single, specific solution, there was consensus on the need for a comprehensive national approach as well as a single coordinating entity to increase efficient

---

[2] See Appendix A for full list of participant organizations.

[3] See Appendix B for detailed scenario information.

communications during times of crisis and enable coordination among stakeholders, possibly working in tandem with an outside non-governmental coordinating mechanism. All participants stressed the need to share more information and reduce classification barriers wherever possible, within a context which respects the sensitivity of sources and methods.

Leadership and Governance Recommendations

- Explore alternatives for establishing a single coordinating entity; possible alternatives could include:
  - An office within the Executive Office of the President with the authority to develop a comprehensive strategy and a unified national vision for cybersecurity
  - A single voice for cybersecurity education, awareness, and alerting within the government (most likely the Department of Homeland Security)
  - A coordinating mechanism that includes relevant stakeholders from government, industry and non-profit organizations
- Expand and enhance forums and mechanisms to maximize information sharing and the expansion of US cybersecurity plans to include international partners

Legal Tools and Operating Principles

Enhanced and updated legal frameworks are required to support the full-spectrum of cybersecurity challenges, including the balancing of privacy with information sharing. The openness of the Internet brings with it the unintended consequence of facilitating the activities of malicious, criminal and terrorist participants. At the same time, the sheer ubiquity of the Internet increases the susceptibility to a range of natural and man-made disasters that can cause irreparable damage. As the scope and complexity of the Internet evolves there is an increasing need for real time suspicious cyber incident reporting and information sharing–this increasing need for reporting may require a change in the culture of trust between government, industry and the public and a refinement of privacy frameworks. Participants recognized the need to revise legal, regulatory and budgetary structures to improve governance across the cyber community. Participants also highlighted the need to remove impediments to industry communication in times of crisis, while simultaneously protecting privacy, proprietary data, innovation and competition. Further, the teams noted that legal frameworks need to keep pace with technology advances and that establishing a "cyber doctrine" is a pressing need. An open dialogue between government and industry to establish an updated governance model to match legal and regulatory frameworks was suggested. The natural tension between the desire to share and the desire to protect intellectual capital was evident, but participants widely recognized the need to share best practices and suggested that increased security may actually be a competitive advantage. Developing an environment for collaboration that is competition-neutral could help incentivize cooperation and increase efficiency in carrying out community-wide cybersecurity initiatives.

Legal Tools and Operating Principals Recommendations

- Institute a review to create a new legal framework with authorities needed to ensure cybersecurity can be achieved without impinging on privacy or undermining national competitiveness while supporting technology innovation
- Continue the dialogue between government and industry to explore the development of a governance model to match updated regulatory and legal frameworks
- Expand industry and academia participation in the early stages of cyber policy development, initiatives and plans

Risk Management and Resilience

The complex, global and interconnected nature of the Internet may require an evolution in thinking about risk management and resilience. The global nature of the Internet requires a cybersecurity framework that extends beyond the borders of the United States. There are no acknowledged global authorities or standards that define the operation of the Internet, and therefore no common, clear and concise definition of a cyber attack. Participants suggested the need to review the structure of the Internet with the understanding that while complete security is impossible, prioritizing and securing core critical infrastructure is feasible. This approach represents the first step in moving beyond the mentality of protecting every asset. Participants recognized the need for an overall shift from a mindset of risk avoidance and management to one of building resilience. One team recommended building the "Internet of the Future" based on performance, security and resilience. To manage the global nature of cybersecurity, teams suggested an international rule of law for the cyber domain and that the United States convene and lead an international forum to create a structure allowing industry and governments to address transnational cyber threats. Government, industry and civil society stakeholders sought to establish expanded and more inclusive forums wherein cybersecurity initiatives and response coordinating bodies and mechanisms were shared. Suggestions were offered to expand and enhance forums for coordinating, sharing and joint operations like the National Communications System (NCS)/National Coordinating Center (NCC) and the National Cyber Response Coordinating Group (NCRCG).

Risk Management and Resilience Recommendations

- Explore the creation of an international forum that preserves privacy, classified and propriety information yet allows the sharing of critical data associated with cyber intrusions and events
- Develop a national-level organization or collective forum to catalog and make recommendations to blunt or mitigate cyber incidents
- Remodel existing forums and include industry in government cybersecurity operations and response coordinating bodies such as the NCRCG
- Establish incentives, standards and best practices for resilience and data integrity with the appropriate balance of security and user convenience

Response Plans and Public Awareness

The complexity of the cyber threat requires a codified and flexible response plan to effectively manage cybersecurity and facilitate public awareness and education. Participants warned that adversaries are taking a holistic approach to the cyber domain, while the response approach

remains fragmented. Some mechanisms to overcome this deficiency could include: pre-planned response protocols with government and industry participation; coordination venues; periodic exercises; identification of stakeholders; demarcated tripwires/triggers; and a cyber checklist for users. One way to codify these protocols would be a "cyber playbook" for interagency collaboration, information synthesis and incident response. Included in this playbook would be a cyber response checklist to include internal and external communications, articulation of decision rights and sector-specific coordination sub-plans. This playbook should be tested, exercised and red-teamed to ensure approaches remain relevant and address current situations. Critical to a cyber national response plan is enhanced education and public awareness of cyber issues. Participants noted that education efforts cannot be delayed until the crisis is at hand and need to be comprehensive and proactive, involving the highest levels of government and industry, as well as media and public interest groups.

Response Plans and Public Awareness Recommendations

- Establish a national public education campaign to expand and increase society and private sector awareness of what is at stake and how they can help
- Establish forums wherein government, industry and academia increases national cybersecurity knowledge
- Form a one-stop clearing house for the public to learn about cybersecurity incidents, trends and solutions
- Explore options for the expansion of cyber elements in the National Response Framework or the creation of a National Cyber Response Framework
- Expand response plans further integrating government, industry and civil society; regularly exercise these plans

Situational Awareness

Greater and more instantaneous cooperation among government, industry and society can enhance cybersecurity situational awareness. Multiple participants focused on creating broad situational awareness of cybersecurity issues. Situational awareness is often hampered by government classification of information, industry proprietary information, restricted information sharing mechanisms and privacy concerns. Developing this situational awareness may require standardizing the types of information that flows between government, industry and civil society. It could also be enabled by building a cyber common operating picture that includes government and industry information and thresholds, tripwires and triggers to allow for real-time reporting of threats and vulnerabilities. This common operating picture would include the development of a dashboard with appropriate cyber metrics. Participants also recognized that the Information Sharing and Analysis Centers (ISACs) and Sector Coordinating Councils are valuable forums for information sharing within sectors, and that a cyber council with well-defined views could aid in the coalescence of information and fusing of data between these entities.

Situational Awareness Recommendations

- Build a common cyber operating picture; possible mechanisms could include:
  - Developing joint government and industry monitoring centers
  - Expanding the US-Computer Emergency Readiness Team's (US-CERT) role as an incident clearing house (i.e., to include a formalized daily dashboard and integrated knowledge across different domains)
  - Reengineering the President's National Security Telecommunications Advisory Council (NSTAC) and National Infrastructure Advisory Council (NIAC)
  - A National Communications System-like model for cybersecurity

Technology and Skills

Cybersecurity solutions can be enhanced by leveraging innovative technologies and the unique capabilities of government, industry, academia and the broader society. The teams noted that as threats continue to propagate at exponential rates, and the speed and agility of academia and private industry should be exploited to develop innovative solutions to overcome these threats. Industry and academia continue to develop cutting-edge cybersecurity tools that must be incorporated into any national solution. A suggested approach was to expand industry and academia participation in the implementation of the Comprehensive National Cyber Security Initiative (CNCI) as an initial step to better use their unique capabilities. Participants also recognized the importance of investment in prevention and monitoring tools. Investments in training to grow a better educated workforce will lead to the development of the human capital necessary to meet the evolving cybersecurity challenges of the future.

Technology and Skills Recommendations

- Expand and accelerate research, development and innovation to improve upon today's cybersecurity practices, tools and integration
- Consider a government-industry function to lead and sponsor network and cybersecurity innovation
- Reestablish U.S. education and vocational skill preeminence in cyber-related technology and scientific innovation

CONCLUSION

While CSI'08 insights indicate there are many aspects of cyber strategy and operations to be explored, the predominate insight was that a new operating model was needed across government, industry and society. The opportunities, challenges and path ahead to ensure a proper level of cybersecurity as well as to reinforce our nation's competitiveness demand a new model of strategies, innovation, network operations and cyber expertise. This model requires closer teamwork among all stakeholders, including our citizens, to collectively promote and enhance the resilience of national digital networks. Business Executives for National Security and Booz Allen Hamilton will further test and refine these insights and recommendations in the coming months and possibly exercise them during a future Cyber Strategic Inquiry in 2009.

APPENDIX A

PARTICIPANTS

Over 230 senior leaders from industry, government, Congress, academia and other sectors participated. Organizations and agencies represented included:

Government	
• Central Intelligence Agency • Department of Commerce • Department of Defense (Joint Staff, USSTRATCOM, Navy, Air Force) • Department of Energy • Department of Homeland Security • Department of Justice • Department of Transportation • Director of National Intelligence	• National Science Foundation • National Security Agency • New York Power Authority • Tennessee Valley Authority • US Government Accountability Office • US House of Representatives • US Secret Service • US Senate • White House Homeland Security Council

Industry	
• Apache Corporation • The Boeing Company • Booz Allen Hamilton • Business Executives for National Security • The Carlyle Group • Cassat Corporation • Cisco Systems, Inc. • Cyveillance • General Dynamics • General Motors • Global Messaging Solutions • Good Harbor • Grant Thornton • Hunt Consolidated Inc. • IBM • J.E. Robert Companies • Juniper Networks	• Lockheed Martin Corporation • L3 Corporation • Mavrick Cyber Defense • McClendon • Microsoft • MorganFranklin Corporation • New Era Associates • Nexant • Paladin Capital Group • Reservoir Laboratories • Sabre Systems • SAIC • Secure Mission Solutions • Southern California Edison • Sprint Nextel • SunGard Data Systems • Symantec • Trust Strategy Group

Civil Society	
• Bloomberg News • Center for Strategic and International Studies • Financial Times • George Mason University	• National Journal • Park University • University of Maryland University College • University of Pennsylvania • Wall Street Journal

APPENDIX B

SCENARIO DETAILS

The simulation consisted of two moves. In the plenary session for each move, all teams were briefed on the general conditions that were being experienced in the simulation. Move 1 focused on detecting and identifying the cyber challenges occurring in the scenario. Move 2 dealt with the need to work collaboratively to mitigate negative effects. During the insights session, participants identified potential innovative solutions and discussed the need for a persistent means–a Cyber Megacommunity–to address the cyber challenges of the future. In particular, participant teams were asked to identify actions they would have taken six months in advance of the crisis and next steps for effectively and openly addressing cybersecurity challenges and opportunities.

Move 1 (December 17th 2008). In this move, an increase in a variety of malicious cyber activities was experienced across government, industry and civil society organizations. Each team was presented with unique information concerning the effects of these events on its sector. Participants were challenged to communicate and coordinate the information that they received to gain an understanding of how and why the incidents were occurring. The incidents were found to be originating from malicious software embedded in thumb drives and CDs that thwarted protections, such as antivirus software, on computers. In the scenario, these devices were distributed as free promotions in several U.S. cities. A second incident affecting telecommunications in the Eastern United States emerged at the end of the move. This incident was the result of a criminal organization running tests of its ability to control the internet's core routing convention, known as the Border Gateway Protocol (BGP). Participants addressed the following questions in Move 1:

- How are the cyber challenges impacting your sector?
- With whom must you coordinate to determine the full extent of the cyber challenges you are facing?
- What coordination mechanisms/venues are you using?

Move 2 (January 5th, 2009). In the second scenario move, cascading effects from the BGP and thumb drive/CD related incidents worsened conditions for the teams and pressured them to work together to mitigate the effects and identify innovative solutions. Incidents described in the second move of the scenario included: denial of service attacks on financial institutions and e-Commerce sites; defacing of the Federal Aviation Administration's website, affecting announcements concerning the cancellation of all U.S. flights; and continued communications outages in the Eastern states. For Move 2, participants addressed the following questions:

- What innovative solutions and/or programs are needed to meet your interests and mitigate the cyber threats?
- With whom must you coordinate to minimize the impacts on your sector?
- What barriers do you face in coordinating? What coordination mechanisms/groups (public/private) may assist in overcoming these barriers?