

Executive Summary

On November 28-29, 2006, the Center for US-Japan Studies and Cooperation of Vanderbilt University hosted the US-Japan Critical Infrastructure Protection Forum (US-Japan CIP Forum) 2006. The event continues an important dialogue that began in 2004 between US and Japanese industries over how to protect critical assets and key resources from harm. The third annual event was another success, featuring esteemed speakers, such as former Secretary of Defense William Cohen, and expert presenters from government and industry of both countries. The Forum also succeeded this year in attracting a number of new US and Japanese sponsors, whose generous and continued support made possible the introduction of simultaneous interpretation. Forum organizers hope that participants took full advantage of the new feature, and that it added value by enhancing understanding and fostering discussion and dialogue throughout the event.

Over 75 individuals representing 46 organizations from the US and Japanese governments and industries met for a day and a half to address the pervasive nature of IT in all aspects of government and business operations, and to share and discuss creative and innovative ways to strengthen and promote a global culture of cyber security. Some of the issues discussed included, the state of and threats to the global information security environment, shifting trends in cyber crimes, impact of emerging technologies and convergence and increasing government activism and its impact.

The Agenda

- Dr. James Richardson of Louisiana State University (LSU) kicked off the event with a presentation that offered Forum participants, who had been thoroughly briefed on the Hurricane Katrina disaster at the 2005 Forum, an update of the recovery and reconstruction efforts ongoing in the city of New Orleans and the Mississippi Gulf Coast region. Gary Sevounts of Symantec Corporation followed, giving a presentation on the vulnerabilities and cyber security gaps in Supervisory Control and Data Acquisition (SCADA) systems that monitor and control operations in critical infrastructure companies.
- As customary, two government officials representing the US Government (USG) and the Government of Japan (GoJ) spoke on recent developments in CIP and critical information infrastructure protection (CIIP) strategies, policies and reorganization. Liesyl Franz of the National Cyber Security Division (NCSD) spoke on recent USG activities in the area of

infrastructure protection touching on the recent nomination of the new Assistant Secretary for Cyber Security and Telecommunications (CS&T), the completion of the National Infrastructure Protection Plan (NIPP) Base Plan and the national cyber exercise, Cyber Storm. Takaaki Saeki of the National Information Security Center (NISC) in Japan introduced progress made over the last year on the First National Strategy on Information Security and the Action Plan for Information Security Measures for Critical Infrastructure. The GoJ has also been actively setting up new mechanisms and frameworks to improve inter-ministry and public-private information sharing and cooperation on information security issues.

- Complementing the presentation given by Ms. Franz, Kenneth Watson of Cisco Systems Inc. spoke from an industry perspective on the developments in public-private partnership initiatives and information sharing mechanisms in the US.
- Former Secretary of Defense William Cohen delivered a remarkable and engaging keynote speech that warned of the duplicitous nature of IT, and its impact on a global economy that is becoming increasingly interconnected and interdependent.
- The afternoon session was kicked off by two presentations that outlined strategies and methods used to prepare for physical and cyber infrastructure incidents. Dr. Masaki Seki of Central Japan Railway Company (CJR) introduced CJR's investment strategy for CIP and a number of security measures undertaken to strengthen infrastructure integrity and resilience against various disaster scenarios. Tom Lehner of the Business Roundtable discussed how executive leaders of top US companies are working on setting up policies to improve information security and network resiliency, as well as mechanisms for information sharing and cooperation before and after major incidents—such as terror attacks or natural disasters.
- Two presentations on the American and Japanese perspective of the impact of convergence on national security and emergency preparedness (NS/EP) communications and network security offered some insight into some of the additional functions and capabilities that the Next Generation Network (NGN) could offer in the future.
- The final eight presentations of the 2006 Forum focused specifically on information security issues, such as globalization of information security, recent trends in cyber crime,

government activism in information security, and introduced innovative solutions for global cyber security.

Lessons Learned

- Preparedness and contingency planning are critical and essential in protecting against physical and cyber threats. Important working relationships should also be firmly established, including roles and responsibilities, before disaster strikes.
- Government intervention in CIP and CIIP issues can be helpful in many ways, but only if businesses and consumers work to educate policy makers and legislators on the realities on the ground and the real issues at hand.
- Government and industry must recognize that best security solutions come from public-private partnerships that identify and act on ways to improve collaboration.
- Information systems will be disrupted and attacked without exception. No one is safe in a global information society that is becoming increasingly interconnected and interdependent.
- Cyber crimes are growing in speed, sophistication and maliciousness across the globe. Government, companies and individuals should do more to protect themselves and their interests from such attacks through increased awareness and consistent application of comprehensive information security strategies.
- There is no “silver bullet” for cyber security. However, effective implementation of holistic security measures, which include the use of new and innovative technologies and varied countermeasures, could help minimize damage and accelerate recovery and reconstitution
- Information security, like cyber criminals, is a moving target. Government and industry should beware of false sense of security engendered by the application of security mechanisms. Information security strategies must constantly be reviewed, reevaluated and updated.

Going Forward

- Although there has been marked progress, more efforts must be made in the area of information sharing across and between governments, government agencies, and industries, because in a global economy every one should be involved in finding security solutions that involve people, processes and technology.
- Public and private leaders of allies and key trading partners should share more information on cyber threat, collaborate on creating an enforcement regime and pool resources for research and development to make cyber space safer for all.
- International collaboration on setting up legal and enforcement mechanisms to capture and prosecute cyber criminals should be given more attention and serious consideration.

A culture of security starts at the top. Leaders of the global information economy, including government officials and key industry stakeholders, should do more to set the tone for the rest of the world. The public should also be made aware that security is not free and should not be taken for granted.