CAPITOL COLLEGE

1927

America on the Cyber Edge

A National Symposium for Pulling Together Silos of Excellence in Information Assurance

Presented by the Innovation and Leadership Institute of Capitol College,
this event took place at the National Press Club in Washington, DC, on March 7, 2008.
It kicked off the start of a cyber-unification campaign for which you can pledge your support.

Dr. Vic Maconachy, Vice President for Academic Affairs

December 7, 1941 marks a "Day of Infamy" in American history. Every year since that day we remember the surprise and anger Americans felt when Pearl Harbor was attacked, seemingly without warning. America also remembers September 11, 2001 in the same light. These two events have much in common; they are clear reminders that our nation can suffer a surprise attack. Subtle warnings and indicators were not recognized in time to prevent those catastrophic events, and in both cases we suffered strategic surprise. As Ariel Levite noted in her book, Intelligence and Strategic Surprise, "…such surprises frequently reveal weakness, vulnerabilities, and pathologies that might not otherwise become apparent." Today, America stands poised for another strategic surprise; cyber attack. Just as in 1941 and 2001, our ability to deter, detect, and respond to attack is an issue of preparedness. Our nation's current state of preparedness for the inevitable cyber attack can best be characterized as silos; silos of opinions, silos of expertise, silos of varying responsibilities and silos of planning. The result is no coalesced action.

There is a leadership void in information assurance. The void exists across portions of America's crucial information infrastructure. Within the executive branch of government we see isolated excellence. The National Security Strategy (2006) declares that National Intelligence must be collaborative, penetrating, objective and far-sighted, while the Intelligence Community's "100 Day Plan" (April 2007) calls for accelerated information sharing. In each instance, there is little regard for intra infrastructure outreach and collaboration. In Congress, several cyber initiatives have been focused on individual and independent cyber areas. These statutory areas include the Clinger-Cohen Act, The Government Performance and Results Act, the Federal Information Security Management Act, and Sarbanes-Oxley. Each independent act is a tremendous step forward in individual arenas, but isolated. Within industry, we see competing Internet Service providers, Software developers, and hardware developers. While competition can be considered the core of the "American way", these instances show that the original call set forth in the National Cyber Security Strategy has not materialized. Information sharing and analysis centers, designed to cut through the communication barriers in the competitive cyber domain, have not taken root. They have not flourished, in part, due to mistrust of government, and also because government-sponsored events are being held subject to the Freedom of Information Act.

In the past, when America has needed independent arbiters, academia has stood up to the challenge. Given the imminent threat poised in the cyber domain, we cannot wait for legislation. We cannot wait for possible intergovernmental collaboration. We cannot wait for cross industrial collaboration. Academia is the perfect locus for pulling all the silos of excellence together. It is time for us to ask questions and seek out solutions collaboratively. In a regional or national cyber event, how will the affected parties cooperate? Who will take command? How will they communicate? How can the American work force be better prepared? These and other urgent strategic problems can be addressed in a collegial and non-threatening fashion.

Go to www.capitol-college.edu/ili and download a personal pledge form to join this national movement.