CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Senate Committee on Commerce, Science, and Transportation

"CYBERSECURITY – ASSESSING OUR VULNERABILITIES AND DEVELOPING AN EFFECTIVE DEFENSE"

A Statement by

Dr. James A. Lewis

Center for Strategic and International Studies (CSIS)

March 19, 2009

I thank the Committee for the opportunity to testify. As America's dependence on cyberspace grows and as the scale of conflict increases, the need to rethink national strategy has become urgent.

The nature of our dependence on cyberspace is not always recognized. We tend to think of cybersecurity as a military or homeland security problem, but our primary interest in cyberspace is economic, and a more secure cyberspace can help to enable recovery and generate growth.

In the early 1990s, there was a debate over the value of information technology. Some economists said that companies had spent millions without noticeable gains in productivity. By the end of the 1990s, this debate was over. There was conclusive evidence that information technology created growth. The reason for the delay between spending and benefit was that companies had to change organizations and their business practices to take advantage of information technology.

Just as companies had to adjust how they operated and were organized, we must now adjust law, regulation and policy. It is no surprise that this adjustment takes time, but in this case, the problem is compounded by the nature of the technology itself.

The internet was designed to provide survivable communications based on rapid and easy connectivity. Its first users were officials who knew and trusted each other. The internet is optimized for easy connection and built on implicit trust. It has changed the world, but it is also deeply flawed. That flaw is security.

The internet as it is currently configured and governed cannot be fully secured. Right now the attackers have the advantage in cyberspace. As a nation, we have not brought the full power of the Federal government to change this.

The United States has done a better job than other countries in cybersecurity. The last twelve months have seen much progress, and the Obama administration has identified cybersecurity as one of the most important issues for national security.

But while the United States has done more than any other nation, we also have more to lose. The risk is not what some cybersecurity proponents would have you believe. We are not talking about explosions, mad hackers, or bringing the United States to its knees in a few hours. The real risk lies in long-term informational damage to our economic competitiveness and technological leadership.

Cyber conflict involves illicit action to penetrate computer networks. This can provide the capability to disrupt key services, as in the case of an opponent who accesses the control system of a critical utility, but the real and immediate threat comes from the theft of intellectual property and the loss of advanced commercial and military technology to foreign competitors.

Cyber conflict is well suited to producing national advantage in the new kind of international competition we face. In this competition, military forces are only one source of power. Economic strength, technological leadership and the ability to innovate are as important. A failure to secure America's information infrastructure weakens the United States and makes our competitors stronger.

Changing this requires two sets of actions. The first is to strengthen our national ability to innovate. A more innovative nation will be stronger and more secure. The second set of actions is to secure the networks upon which we rely for commerce, innovation and security.

Let me give you two examples of how cybersecurity, innovation and the economy are connected. The recent stimulus bill provided a significant increase in funding for research in the hopes that this would increase innovation in the United States and with it, growth and competitiveness. This is good, but if we do not improve cybersecurity, new Federal funding to increase research and innovation will be a subsidy to foreign industry as much as our own.

Another stimulus-related problem involves the Smart Grid, which makes innovative use of advanced meters. If the new "smart" grid is not secure, it can be hacked and used to disrupt the delivery of electricity.

In the past, we viewed cybersecurity as a technical problem. We can no longer afford this. Cybersecurity requires using all the tools of U.S. national power – diplomatic, military, intelligence, law enforcement and economic policy. In 2007, CSIS established a Commission of recognized experts to develop a comprehensive cybersecurity strategy. Our recommendations called for new kinds of deterrence, serious international engagement, the use of regulation, better authentication of identity, building human capital, and White House leadership.

A national strategy that is not comprehensive will fail – we have learned this the hard way, from our previous national efforts. Cybersecurity will require a coordinated effort by many agencies. We do not currently have a mechanism to do this, although the Obama Administration's sixty-day review of cybersecurity policy may provide one.

Congress can focus Federal efforts on the economic benefits of cybersecurity and ensure that regulatory efforts give full weight to cybersecurity – something that is not now the case. It can ensure that the Department of Commerce, which has a crucial role, makes cybersecurity a priority. Finally, Congress can begin the daunting task of modernizing legal authorities, many of which were written decades ago for simpler technologies.

My testimony has discussed how information technology has brought great benefits, but that these are accompanied by unavoidable costs. We have an opportunity to secure cyberspace and use it to provide renewed economic growth, more efficient government, and stronger national security. These are attainable goals, and the nation that finds new ways to use cyberspace securely will gain competitive advantage.

I thank the committee and will be happy to take any questions.