Testimony
Senate Committee on Homeland Security and Governments Affairs
"Cyber Security: Developing a National Strategy"
James A. Lewis
Center for Strategic and International Studies
April 28, 2009

I thank the committee for the opportunity to testify. Among the many difficult challenges America faces this year, cybersecurity deserves special attention. If America continues to fail in securing cyberspace, our most important national economic and security interests will suffer critical damage. We must organize and equip ourselves for conflict in cyberspace. Major agencies have key roles to play in this, but their efforts must be coordinated and comprehensive to be effective.

Conflict in cyberspace is best seen as a steady erosion of America's technological, military and economic leadership. This erosion is accompanied by the almost certain risk that our opponents will use cyber attacks against critical infrastructure in the event of a conflict with the United States, but the central problem before us involves espionage and crime. These problems – espionage, crime and risk to critical infrastructure – will never go away, but they can be better managed and the degree of risk can be reduced by coordinated government action.

A brief summary of the current state of our efforts to protect cyber networks is that they are inadequate. This is not a criticism – many people have worked hard in recent years to improve cybersecurity, but we are starting late and we have not done enough. Our opponents are the intelligence and military services of hostile nations and a set of shadowy but highly skilled cybercriminals. They are well resourced, inventive and experienced, and have successfully exploited network vulnerabilities in the United Sates

The topic of this hearing – developing a national strategy – is very timely. The United States needs a truly comprehensive national strategy that addresses all dimensions of the cybersecurity problem and engages all stakeholders. There is a national strategy, the 2003 National Strategy to Secure Cyberspace, but it is generally perceived as inadequate in part because as it relied to heavily on voluntary efforts. There is also the 2008 Comprehensive National Cybersecurity Initiative, but it was not truly comprehensive in that it focused on securing government networks.

In December of 2008, the Center for Strategic and International Studies Cybersecurity Commission laid out a series of recommendations for a comprehensive national approach to cyber security. We called for the creation of a strong White House cyber advisor with clear authority over policy and, in coordination with the Office of Management and Budget, over budgets related to cybersecurity. One reason that previous administrations have failed to secure our nation's digital infrastructure is that they have divided responsibility for cybersecurity among many agencies and White House offices. Our opponents exploit these divisions. We proposed creating a new White House office for cyberspace to work with the NSC to manage the many aspects of securing our national networks, consistent with privacy and civil liberties, and to help begin the work of building an "information age" government based on the new, more collaborative organizational models.

A comprehensive national strategy for cyberspace would use all the tools of U.S. power in a coordinated fashion – international engagement and diplomacy; military planning and doctrine, economic policy tools and regulation, and the involvement of the intelligence and law enforcement communities. A comprehensive approach should include a public doctrine for cyberspace that makes clear to our foreign partners and adversaries that the cyber infrastructure of the United States is a vital asset for national security and the economy and that the U.S. will protect it, using all instruments of national power, in order to protect national security and public safety, ensure economic prosperity, and assure delivery of critical services to the American public.

Our report contained recommendations on many other important elements for improving cybersecurity, including the need for increased education and training, for the modernization of outdated laws, greater use of acquisitions authorities to drive product improvement, and for better authentication of online identity within government and critical infrastructure. A truly national approach must address these issues if it is to succeed.

We also called out the issue of market failure. One of the reasons earlier efforts have not succeeded is that they ignored the disconnect between market forces and national security. We have been waiting for more than a decade for the market to deliver the innovations needed to secure cyberspace. While there has been some improvement, there will never be enough without active White House leadership that is grounded in a clear vision for a secure digital future.

There is some chance that several of our recommendations will be adopted, to some degree by the new administration. As you know, it has recently concluded a sixty day review of cybersecurity policy, and while few public details have been released, it is clear from public statements that he White House will play a greater role in organizing cybersecurity policy, that there will be greater attention to international engagement and to relations with the private sector, and closer coordination among agencies. These are all positive developments if they indeed turn out to be the direction that administration policy takes.

My hope would be that the sixty-day review leads to a strong White House cyber advisor with clear authority to set policy and help guide budgets. But there is an intense and unfortunate policy debate within the administration over how much authority the cyber advisor should have and how strenuously the U.S. should protect its cyber networks. I say unfortunate because our opponents are not waiting sixty days to attack us.

While policy and coordination must be led from the White House, implementation and operational activities should fall upon the agencies. The key agencies for cybersecurity are the National Security Agency and other Intelligence community components, the Department of Homeland Security, the Federal Bureau of Investigation, the Department of Defense and the Departments of State and Commerce. Each of these agencies has a different sphere of responsibility, although there is some overlap, and different expertise.

Operational responsibility for cybersecurity falls primarily upon NSA, FBI and DHS. NSA has the expertise, the experience and the resources to defend cyberspace as part of a larger and comprehensive national strategy. Its efforts focus on securing military and intelligence networks for the government. FBI has a national presence, strong legal authorities for dealing with cybercrime and has reorganized itself to give cybersecurity greater prominence in its law enforcement mission.

DHS's role is more complex. In the previous administration, the White House assigned DHS the lead role for cybersecurity, but this was beyond its competencies. DHS is not the agency to lead intelligence, military, diplomatic or law enforcement activities. This does not mean that DHS does not have an important role, however and properly scoping the role and responsibility of DHS and then providing adequate resources for those responsibilities is an urgent task for this administration.

DHS has the responsibility for securing critical infrastructure. It also has the responsibility for securing civilian government networks – the "dot gov" networks. It is beginning to build the capabilities needed to carry out these missions. Building this capability requires sustained investment in facilities, technology and in the DHS cyber workforce. At the moment, these are inadequate to the task and increased allocations for cybersecurity are essential.

Some of the resource challenge revolves around the acquisition and use of technologies to better secure civilian government networks. The CNCI had a program named "Einstein" to provide this surveillance. A year ago, DHS introduced "Einstein II," an upgraded network surveillance system. Neither Einstein nor Einstein II are adequate to the task, and while DHS plans further upgrades (culminating in "Einstein IV"), the immediate question is whether in the interim, there are ways to take advantage of NSA technologies to perform the "dot gov" surveillance mission that provide adequate safeguards for privacy and civil liberties. This is of course a sensitive topic - NSA has the capabilities; DHS has the responsibilities and authorities, and there are compelling constitutional reasons for restricting NSA's role. That said, and despite the worries about giving NSA too large a role, it would be a serious error for DHS not to find ways to take advantage of NSA's skills and capabilities for defensive missions at a time when our government networks are under serious, sustained and successful attack.

DHS may also want to consider some reorganization to improve its performance in cybersecurity. Perhaps the most immediate of these steps would be to merge USCERT and the National Communications System (NCS) and its components into a single entity. It no longer makes sense to separate cyber and telecom.

DHS's cyber functions are part of its larger National Protection and Programs Directorate. This Directorate faces a strategic challenge in better integrating the plans for physical infrastructure and cyber infrastructure protection and resiliency, and for making these plans more focused and less cumbersome. The 2009 National Infrastructure Protection Plan, although it is 188 pages, could be improved with a more precise definition of critical infrastructure, a better assessment of risks and a greater focus on action.

As part of its critical infrastructure responsibilities, DHS is the Federal interface with private sector critical infrastructure owners and operators. There are a plethora of groups; none are sufficient. DHS may wish to look at the Department of Defenses "Defense Industrial Base"

(DIB) effort as a model for a new approach to partnership and information sharing. While the DIB does not translate exactly to DHS's responsibilities, it has had some success and DHS should examine it closely.

The overall question of how to improve cybersecurity in critical infrastructure is a difficult one. We know that current levels of protection are very uneven. Changing this raises troubling questions of regulation and investment. The United States has previously relied on voluntary action by critical infrastructure to provide adequate security, but to quote the former chairman of the Security and Exchange Commission, Christopher Cox, a longtime proponent of deregulation, "The last six months have made it abundantly clear that voluntary regulation does not work. A new Federal approach to cybersecurity must elicit actions from the private sector that it would not otherwise perform.

Government intervention in response to market failure can include regulation (or the threat of regulation) or subsidy. Both have limitations, but both are preferable to inaction. DHS does not now have regulatory authority for most critical infrastructure, and rather than giving DHS new and expansive authorities, it might be better to use exiting agencies, such as the FCC, FERC, the NRC and others, to guide their sectors to better cybersecurity.

Efforts by DHS alone cannot improve cybersecurity. The United States needs to develop a strong offensive capability and place this capability in the context of a well-defined chain of command leading up to the President. An offensive capability can contribute to a cyber-deterrent and help inform out own defensive efforts. The United States must shape the international environment to improve cyberspace, by increasing multilateral cooperation in law enforcement to shrink the sanctuaries for cybercrime that currently exist. We need to expand relationships with our allies for mutual defense in cyberspace and work with the international community to develop normal and sanctions for hostile action in cyberspace – no nation should be able to brag, as Russia has, about its exploits in Estonia and Georgia and not face some consequence. Federal incentives and regulation can help create the innovation we lack in cybersecurity, and federal investment in research that is complement private sector efforts can help provide the long-term basis for secure networks.

This is a complex agenda. It will not be easy to achieve. However, the United States is in a very unfortunate situation. We have taken better advantage of cyberspace than our competitors have, and this has provided real economic benefits. Our reliance on cyberspace holds the potential for recovery and future growth. However, the combination of greater reliance on cyberspace and inadequate attention to security has left us more vulnerable than our opponents. If we cannot change this, the power and influence of the United States will shrink, and our prosperity and security will be damaged. Congress and the executive branch have the opportunity to avert this damage if we act now.

I thank you for the opportunity to testify and will be happy to take your questions.