Senate Committee on Commerce, Science, and Transportation
Cybersecurity – Assessing Our Vulnerabilities and Developing an Effective Defense
March 19, 2009

James A. Lewis
Center for Strategic and International Studies

I thank the Committee for the opportunity to testify on vulnerabilities and effective defense in cyberspace. As America's dependence on cyberspace grows, and as the scale and pace of conflict in this new venue increases, the need to rethink national strategies has become urgent. The free and secure use of cyberspace has become, like freedom of the seas, a vital national interest for the United States. This Committee can play an important role in developing and guiding an adequate national approach to securing cyberspace.

The nature of our dependence on the use of cyberspace is not always recognized. We tend to think of cybersecurity in military terms, or as a problem of homeland security, but this is inadequate for understanding the scope of the problem. Networked, digital information technology provides the infrastructure for new ways to organize, interact and create wealth – actions that can now take place in cyberspace. Information technology lies at the center of an immense and ongoing transformation in the global economy, in politics and society, and in military affairs. It has transformed how people work, altering business models, supply chains, customer interactions and production. The use of cyberspace has become a central element in both economic and national security.

You may recall that in the early 1990s, there was a debate over the value of investing in information technology. Some economists noted that American companies had spent millions of dollars on information technology without any noticeable gains in productivity. The promise of information technology, they asserted, was a mirage. The excesses and rhetoric of the dot-com bubble only contributed to this perception.

But by the end of the 1990s, this debate was over. There was conclusive evidence that spending on information technology brought economic benefit. Information technology made a significant contribution to American GDP growth – perhaps as much as a third of total GDP growth. It turned out there was a lag, a delay between spending on IT and the increase in growth. The reasons for this delay were that companies had to figure out how to change their organizations and their business practices to take advantage of the new and more efficient processes enabled by IT. New technology layered over old organizations does not provide much benefit.

We can draw two conclusions from this story. First, we are barely into our second decade when it comes to exploiting the advantages that digital network technologies provide. If this story was about cars, we have moved from the Model T, introduced in 1908, to the Model A, which appeared in 1927. This is progress, to be sure, but we are only at the beginning of the story. We have not exploited the full potential of the new technology for recovery and for future growth.

Second, just as there was a lag as companies took time to adjust how they operated and were organized to make use of the new technologies, we are facing a lag in adjusting law, regulation and policy. To continue the car analogy, if the economy as a whole is moving towards the

Model A, the Federal government is still comfortable driving a Model T. The difficult task of modernizing the Federal government will challenge both the administration and the Congress.

A common element links both business and governmental stories together. That element is security. It is no surprise that a new technology that has immense economic and political effect requires adjusting our security policies, and that we have lagged in doing so, but in this case, the problem is compounded by the nature of the technology itself.

The story of the internet is well known. It was designed to provide survivable communications based on rapid and easy connectivity across a nation-spanning network. Its initial users were scientists and military officials, small communities that knew and could trust each other. The internet is an open network 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. Changing this to gain the further advantages offered by information technology will require a restructuring of governance, practices and standards. Right now, however, the advantage lies with the attacker. This has been apparent for years, but as a nation, we have not brought the full power of the Federal government to bear on the problem, and what power we did bring was applied in a fragmented and incoherent manner.

This is a harsh statement, and if it is any consolation to the committee, the United States has done a better job than any other country in cybersecurity. The last twelve months have seen more progress toward securing cyberspace than any previous year. More importantly, the Obama administration has identified cybersecurity as one of the most important issues for national security and has begun to move forward.

However, we should bear in mind that while the United States has done more than other nation in terms of security, this is in no way adequate. One reason for this can be termed asymmetric vulnerability. We have more to lose than our opponents do. We are more reliant on information technology and networks, and it is a greater source of our comparative advantage in economic competition and in national security. As a nation, we have been quicker to take advantage of the internet and offer a "target-rich" environment to our opponents, who currently rely on it less.

Over time, this will change. No country can ignore the benefits of digital networks if it wishes its economy to be competitive, its researchers effective and its nation to be secure. In the interim, however, the United States is at greater risk than any other country. The risk is not what some cybersecurity proponents would have you believe. We are not talking about explosions, mad hackers, fatalities, or bringing the United States to its knees in a few hours. These claims are best left to Hollywood – entertaining, but a poor guide for policy. The real risk lies in the long-term informational damage to our economic competitiveness and technological leadership.

Our primary opponents in cyberspace – and we are already in a conflict even if it often takes place largely outside of public view – are nation-states and organized criminals (who sometimes work at the behest of nation-states). Cyber conflict involves illicit action to penetrate computer networks. These penetrations may provide an opponent the capability to disrupt the delivery of key services, as in the case of an opponent who surreptitiously accesses the control system of a critical utility or network. This potential threat is one that we need to guard against. The real and immediate threat from conflict in cyberspace, however, is illicit action to obtain access to sensitive information – in other words, espionage and theft.

That cyber incidents are not comparable to attacks involving the use of force does not mean that they are not damaging. Clearly, there are potential military advantages that come from greater knowledge of an opponent's intentions and capabilities, access to critical military technologies, and the ability to disrupt and slow decision-making by introducing uncertainty provides immediate advantage. Action in cyberspace has become part of modern warfare.

More importantly, cyber conflict is well suited to producing national advantage in the new kinds of competition that will shape international relations in the future. In this competition, military forces are only one source of power. Economic strength, technological leadership and the ability to innovate will be as important as military force in creating national power, particularly in competition with the rising nations who wish to reduce U.S. influence without resorting to open military conflict. The primary damage to U.S. national security and economic strength from poor cybersecurity comes from the theft of intellectual property and the loss of advanced commercial and military technology to foreign competitors. A failure to secure America's information infrastructure weakens the United States and makes our competitors stronger.

2007 was perhaps the worst year for the United States when it comes to cybersecurity – it may have been the long-awaited Electronic Pearl Harbor, despite the lack of explosions or casualties. The Secretary of Defense's unclassified email was hacked. The Department of Commerce's bureau for high tech trade had to go off-line after its networks were penetrated. Foreign entities penetrated the networks of the Departments of State and Energy, NASA and other federal agencies, along with networks at federal contractors, the defense industry and major companies. It is interesting to note that in the same period the governments of the United Kingdom, France and Germany also experienced major cyber incidents, which they attributed to China.

In response, the Bush Administration created the Comprehensive National Cybersecurity Initiative (CNCI). While the initiative made progress in securing Federal networks, the CNCI had major drawbacks. It started too late, in the last year of the Bush Administration. It was over-classified. Most importantly, despite its name, the Comprehensive National Cybersecurity initiative was not comprehensive. The CNCI focused on government networks, and while this is important, it is inadequate. Cyberspace is a global commercial network. The CNCI did not have an international component, it did not adequately address how to secure critical infrastructure, and it ignored the "dot.com" space where most commercial activity takes place. These were serious shortcomings, and they point to crucial areas for work for the new administration.

Despite the CNCI, intense economic espionage made possible by the internet is eroding America's technological leadership and economic strength. Repairing this situation requires two interrelated sets of actions. The first is to strengthen our national ability to innovate. Innovation is the process of coming up with news ideas, goods, and services. It has become a central element in economic competition. A more innovative nation will be stronger and more secure as it will have a stronger economy and better technology. A purely defensive strategy will not succeed. The second set of actions is to secure the networks upon which we rely for commerce, innovation and security. Two examples help demonstrate how these actions are related.

There is a strong connection between innovation and information technology. Information technology lowers the cost of acquiring information and creating new knowledge. It extends human capabilities to count and observe. Digitizing knowledge and research increased the productivity of the innovative efforts. Recognizing that research is a fundamental source of innovation, 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 a good idea, but there is one important caveat to bear in mind. Much of the new information created by the additional funding for research will be stored in computer databases. These databases are usually networked and connected to the internet. That means they are vulnerable to penetration and the information stored on them accessible by others. The end result, if we do not improve cybersecurity, is that 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 an infrastructure project, the Smart Grid. Smart Grid makes innovative use of advanced meters to better manage the flow of electricity. These new meters use computer technologies to make our national electrical network more efficient. Unfortunately, if the new “smart” meters are not secure, they can be “hacked,” taken over by attackers, and used to disrupt the delivery of electricity. If the smart grid is built to existing standards, however, it will not be secure. Worse, the United States does not have a process that could deliver in a timely fashion the new standards needed to guide the construction of secure smart grids. Years of underinvestment in infrastructure have put us in this unfortunate situation.

These two examples show how recovery and growth, innovation and cybersecurity are intertwined. In the past, we viewed cybersecurity as a problem somehow separate from larger national issues, something that could be safely ignored or left for consideration by technical experts. This is no longer the case. Since the information infrastructure is now a central pillar of our economy and since the untrammeled use of cyberspace is crucial for economic and military security, we cannot ignore it nor can we approach it as a technical problem. An effective policy for this complicated strategic problem will engage many different elements of the American government and requires using all the tools of U.S. national power – diplomatic, military, intelligence, law enforcement and economic policy. A national strategy that does not take a comprehensive approach will fail – we have learned the hard way, this from the experience of our previous national efforts, in 1998, 2003, and 2007.

CSIS established a Commission of recognized experts in 2007 to look at what actions the Federal government could take to improve cybersecurity. The Commission released its report in December of 2008. The report laid out the elements of a comprehensive strategy. This recommended strategy called for better integration of offensive and defensive capabilities to create new modes of deterrence. It recommended expanded international engagement to establish norms and partnerships for securing cyberspace. It concluded that a voluntary, industry led approach to national security was insufficient and that the Federal government must require mandatory action to improve cybersecurity. It called for improving our ability to authenticate digital identities. Finally, the report determined that the United States needs a coherent and comprehensive organizational and policy framework to secure cyberspace.

Reorganizing government and adopting new practices to enable and secure the use of cyberspace is one of the most difficult tasks in this comprehensive approach. The United States will require a coordinated effort by many agencies. We do not currently have a mechanism to do this, although the sixty-day review of cybersecurity policy the Obama administration is undertaking may provide one. None of the problems we face in cyberspace are unsolvable, but they require a comprehensive approach that has not been used in the past. In the litany of errors and omissions that accompanies any account of previous U.S. cybersecurity policies, the failure to seek broad international engagement or to use the regulatory powers of the Federal government head the list (along with disorganization and diffusion of effort). You have an opportunity to change this, working with the executive branch and the private sector.

One important contribution that Congress can make is to ensure that a national approach to securing cyberspace is forward looking. Congress can focus Federal efforts on the importance of the economic and commercial aspects of cybersecurity, and ensure that the regulatory efforts of important agencies like the Federal Communications Commission give full weight to cybersecurity – something that is not now the case. It can ensure that elements of the Department of Commerce which have crucial roles in securing cyberspace – the National Institute of Standards and Technology and the National Telecommunications and Information Administration – make security a priority. Finally, one of the most daunting tasks before Congress lies in modernizing the range of legal authorities concerning privacy, security, infrastructure protection and the management of digital identities, many of which were written decades ago for simpler technologies and times.

In considering these issues, it is worth recalling that the United States has used a market-led approach to cybersecurity for more than a decade. It has failed us. The CSIS Commission report concluded that market forces alone would not provide adequate national security. This is a major departure from previous thinking, which tended to approach the question of regulation timidly and to defer to business interests on matters of national security. Badly designed regulation is a hindrance but no regulation in situations where there is market failure is even worse. The CSIS Commission proposed a new regulatory approach based on standards and an avoidance of prescriptive rules. The Commission's recommendation is to begin with regulation for critical infrastructure – if infrastructure is truly critical, we should not be shy about mandating action to secure it.

My testimony has attempted to show that information technology has brought great benefits, but that these are accompanied by unavoidable (albeit smaller) costs that we have not done well in managing. Our goal is to take the open network we have inherited and sufficiently secure 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. With a unified and forward-looking effort, that nation can be the United States.

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