Testimony
Committee on Oversight and Reform
Subcommittee on Management, Organization and Procurement
United States House of Representatives
"Cybersecurity: Emerging Threats, Vulnerabilities and Challenges in Securing Federal Information Systems"
James A. Lewis
Center for Strategic and International Studies
May 5, 2009

I thank the Committee for the opportunity to testify and I would like to begin by apologizing, as I will not have any of the more dramatic prognostications that often accompany a discussion of the emerging threats, vulnerabilities and challenges. My own view is that it is can be a handicap to developing adequate policy to go about saying that the end is near or that tiny bands of hackers can wreak havoc on a scale or September 11 or Pearl Harbor. They cannot, but that is not to say there is no damage being done to the U.S. in cyberspace. My fear is that when we predict the end of the world, and it does not happen, people lose interest or think the problem is not serious yet in some ways it is not an exaggeration to say we are in crisis. Let me give two examples.

At the start of World War Two, a British carrier was caught off the coast of Norway by two German battleships and sunk. How did the Germans know where the carrier would be? The Germans knew because they had broken the British navel code and were listening in on British naval networks. This could happen again, to us instead of the British, as our prospective opponents can access our networks.

At the end of World War Two, the United States had a monopoly on the atomic bomb. The Soviet Union was able to steal the information that had cost the Americans billions of dollars to develop. The Soviets exploded their first bomb a few weeks after the CIA predicted it would take them years to build one. We are experiencing something similar today when foreign opponents can steal technology without even leaving the comfort of their offices. The United States is unwittingly sharing its intellectual property and technological secrets with hackers around the world, at little or no cost to them.

If you were to look for common themes in these incidents, they would be an unwillingness to recognize our own vulnerabilities or admit how deeply we have been penetrated, and a certain belief in our own superiority over our opponents. I still hear people say that America is the internet leader and that our technology is the best. That was possibly true even as late at ten years ago, but is no longer the case. We may still be first among equals but on bad days, I am not even sure about that.

And we have had many bad days. How did we get end up with these problems? First, the effusion of joy that greeted the commercialization of the internet created its own perverse ideology, that government had no role in cyberspace, that it was too slow and too cumbersome and that any intervention would only choke the wonderful flow of innovation. There is some truth to this, but it is not true for public safety or national security. Second, there was a belief that the market would deliver adequate protection. While a well-regulated market is the most

efficient way to organize economic activity, the market has always been recognized as inadequate for national security. Even Adam Smith, the 18th Century British economist, wrote in the Wealth of Nations that markets would not provide for national defense. But we have not.

Second, the technology of cyberspace was not designed to be secure. The goal of the early designers was to ensure rapid, efficient connection. They did not worry about trust and authentication of identity. One result is that a system designed for a few thousand scientists in the United States is, after twenty years, now used by hundreds of millions of people around the globe. It is possible that the Internet, as it is currently architected, can never be secure.

Third, the same forces that led to the rapid growth of internet users have also contributed to the rapid growth of internet-based applications in other industry sectors. Our economy has become more efficient and more productive because many functions – from stocking milk in grocery stores or that runs automatic teller machines to the control systems of our electrical grids – now use digital technology and IP based networks.

This is a real advantage. The use of digital network technologies like the internet has given America an advantage over our economic and military competitors. More importantly, the greater use of digital network technologies will accelerate recovery and growth in the future. In the last five years, our economy has become dependent on cyberspace in ways that are not generally recognized and in the future, it will be even more dependent. The question before us is whether we can find a way to use these technologies securely in order to reap their benefits without crippling loss.

The answer to this question, so far, is no. It is not a technological problem, although there are difficult technological problems to solve. It is a political problem. We are on our fourth attempt to improve cybersecurity. In 1998, Presidential Decision Directive 63 order agencies to begin to cooperate to protect critical infrastructure. PDD-63 still shapes policy, but government and commercial networks are no more secure than they were a decade ago. The 2003 National Strategy to Secure Cyberspace laid out a vision for the secure use of cyberspace, but it was crippled by fighting over turf and ideology and ended up being largely an expression of faith that in the private sector. The 2008 Comprehensive National Cybersecurity Initiative is more interesting. While it was not comprehensive, while it faced the usual turf battles and ideological hurdles, and while it was started far too late in the Administration, it contained several serious and useful initiatives. Finally, the Obama administration began its tenure with a sixty-day review of cybersecurity policy conducted by the National Security Council.

What has changed that made the U.S. start to take the threat more seriously? Beginning perhaps five years ago, U.S. dependence on cyberspace became crucial as we wove network technologies deeply into our daily lives and activities. Our opponents realized this and exploited it unmercifully. 2007 was a year of horror for America's defense of cyberspace and the CNCI was a late effort to respond to the crisis.

This sounds dramatic, and it is important to remember that the disaster was an intelligence disaster for government and a financial disaster for businesses, not the sort of story we see in films involving flames, explosions and death. Just because something is hidden from sight does

not mean it is not a disaster and a simple listing of the press accounts of the battle in cyberspace since spring of 2007 gives an idea of the scope of the crisis:

-- The Secretary of Defense's unclassified email was hacked by unknown foreign intruders.

-- NASA was forced to block email with attachments before shuttle launches out of fear they would be hacked, and Business Week reported that the plans for our latest space launch vehicles were obtained by unknown foreign intruders.

-- The National Defense University had to take their email systems offline because of hacks by unknown foreign intruders.

--FAA computer systems were hacked and, as the FAA increases its dependence on modern IP-bases networks, the risk of the intentional disruption of commercial air traffic has increased.

-- The Department of Commerce had to take the Bureau of Industrial Security's networks off line for several months. This Commerce Bureau reviews high tech exports and its networks by unknown foreign intruders.

--The Department of State's networks were hacked and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards and spent the night carting off file cabinets it would be an act of war, but when it happens in cyberspace, we barely notice.

--The databases of both the Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

-- Classified networks at DOD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and resecure the networks.

-- Contractors at DHS and DOD had their networks hacked, as a back door into agency systems.

-- The networks of Congressional offices were hacked by unknown foreign intruders. The incident I know about involved offices with an interest in human rights or Tibet.

-- Canadian researchers found a computer espionage system that they attributed to China implanted on the government networks of 103 countries.

-- Estonia and Georgia had their cyber networks attacked by unknown foreign intruders, most likely at the behest of the Russian government. These were more like cyber riots than crippling attacks, and the Estonians responded well, but they created a wave of fear in countries like the U.S. that depend heavily on cyberspace.

-- Cybercrime became the most profitable and least risky form of bank robbery and credit card fraud, costing our economy tens of millions of dollars. If a robber walked into a bank with a gun and stole a million dollars, it would be all over the front page, but in cyberspace, there are only

whispers – and there have been a few cybercrime incidents involving losses of a million dollars. A smart cybercriminal has zero chance of being caught and prosecuted.

-- The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.

--I am told that American, European and Japanese companies are experiencing significant losses of intellectual property and business information, but this cannot be confirmed in an unclassified setting.

--Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some of my colleagues would go into the new administration and may have thought it might be interesting to read their emails beforehand.

-- And of course, you have seen the Wall Street Journal articles on the vulnerability of our power grid to cyber attack – a vulnerability we are busy increasing - and the intrusions into some F-35 databases by unknown foreign intruders.

All this in a single year, and there are probably some that I have missed and others we have not even found. It is impressive, and I expect that several unknown foreign intruders have received medals and promotions while some cybercriminals in Eurasia have entered the ranks of the rich.

To take a step back, the U.S. faces "asymmetric vulnerability" in cyberspace. We are as good as our opponents when it comes to offense and espionage, but we are also much more dependent on cyberspace than they are and our defenses are too weak. We are a "target-rich environment." Being the richest economy – even after the crash – and the nation with the most advanced military technology means we are number one on everybody's target list for hacking.

The change in cybercrime is one example of how the threat has increased. Cybercriminals are not amateurs, they are not teenagers in a garage in Mendocino. Cybercriminals now include some of the most skilled programmer in the worlds. They are well organized – there are cybercrime websites and chatrooms that are closed to the public, where you can buy advanced hacking tools, rent botnets (collections of zombie computers to use in an attack) or buy credit card data , bank account, and personal information in bulk – when I say bulk I mean in lots of a thousand or ten thousand – the more you buy, the lower the price. Everything cybercriminals can do, the best foreign intelligence and military services can do as well, if not better.

We cannot simply arrest these people in most cases for two reasons. First, attribution is very difficult – this is why the term unknown foreign entity appears so often n the list above. Criminals and attackers exploit the anonymity of the internet and it is a common trick to attack from one country but make it look like the attack came from somewhere else. Second, the most skilful cybercriminals live outside our borders, often in countries that are de facto sanctuaries for cybercrime. They are outside our jurisdiction and these countries will not always cooperate in law enforcement cases. There is an international treaty on cybercrime – the Council of Europe's Cybercrime Convention, but many nations, including China and Russia, have refused to abide by

it. If we cannot catch sophisticated cybercriminals, it is even harder to catch intelligence agents who are protected by their governments.

There is no easy solution to this problem but it is not unsolvable. In December 2008, a CSIS Commission on Securing Cyberspace issued a report with a number of recommendations for how to improve the situation. Our two primary recommendations were to establish strong leadership in the White House by providing the President with a single cybersecurity advisor to guide policy and budgets and to develop a truly comprehensive national strategy that used all the tools of American power. Currently, we have neither. Many large agencies have important roles in and left to their own devices, they will not cooperate to the degree that is needed for cybersecurity. Only the White House can provide national the required vision, based on Presidential Strategy and Directives, and ensure policy coordination. To summarize our other recommendations:

-- Create a comprehensive national security strategy for cyberspace that uses all the tools of U.S. power in a coordinated fashion – international engagement and diplomacy; military planning and doctrine, economic policy tools and the involvement of the intelligence and law enforcement communities. A comprehensive strategy must involve engagement with other nations, both our allies and our opponents, to see how much agreement we can reach on securing cyberspace. This will be a long-term process, but it needs to begin now.

--Publish a public doctrine for cyberspace. The President should state publicly 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. This needs to be said clearly and visibly to put our opponents on notice, not buried in a classified document or in some anonymous official report.

--Use regulatory authorities to ensure that the delivery of critical services can continue when we are attacked. The CSIS report identified four sectors – telecommunications, energy, finance and government services – as the most critical for cyberspace. Securing them will active government policies where the government can compel action when necessary to provide for public safety and national security. Public safety and national security are a government mission and cannot be left to voluntary private efforts.

--Mandate strong authentication of identity for both people and devices for access to the networks for telecommunications, energy, finance and government services**.** Strong authentication of identity for digital networks can significantly improve defense, if it is done in a way that protects privacy and civil liberties.

--Use acquisitions policies and rule to encourage the development and use of products and services that are secure, based on standards and guidelines developed in partnership with industry.

--Build human capital by expanding research, training and education for information technology and cybersecurity.

-- Refocus and strengthen public-private partnerships and focus them on action, not information sharing.

These recommendations lay out a comprehensive approach to cybersecurity, but recommendations are most valuable when they are implemented. This Committee, along with other committees and with the executive branch, have an opportunity to improve cybersecurity in the United States. Improving Federal government security is an important part of this. Oversight to ensure that cybersecurity becomes a priority for the Federal government is crucial. Too often, we hear that an agency will say that its mission – whether it is health care or air traffic control – is more important and cybersecurity is a lesser priority that can be put on hold Congress can help change this.

Federal acquisitions are a vital tool for improving network security. One of the strongest elements of the CNCI was an initiative called the Federal Desktop Core Configuration. This initiative made vendors sell securely configured products to the government. There were some complaints about the FDCC, but this was more about process than the actual policy, and expanding this initiative would markedly improve the security of government networks

Homeland Security Policy Directive-12 required federal agencies to use secure network credential for all of their employees. This would make it harder for anonymous strangers to penetrate government networks. Although all agencies were expected to comply with HSPD-12 by December 2007, only about a third have actually done so.

The Federal Information systems Management Act desperately needs to be modernized. It currently focuses on compliance with written plans and an agencies FISMA score actually tells us nothing about the security of its networks. A draft bill just introduced by Senator Carper in would greatly improve FISMA by focusing it on real security measures. Along with the FISMA bill, draft legislation introduced by Senators Rockefeller and Snow, by Senator Feinstein on data breaches, and by Senator Lieberman and Representative Thompson on securing the electrical grid have all begun the process of providing a sound legislative structure for a new American effort to secure cyberspace.

In addition to the legislative activity, the White House review of cybersecurity policy has concluded and a new policy may be announced shortly. This was a very intense effort that covered an amazing amount of material in a very short time. While few public details have been released, it appears that the White House will play a greater role in organizing and leading cybersecurity policy and ensuring closer coordination among agencies, and that there will be greater attention to international engagement and to relations with the private sector. If the review produces a strong White House cyber advisor with clear authority to set policy and help guide budgets and a commitment to develop a comprehensive strategy the United States can begin to remedy our serious weaknesses in cybersecurity.

I began this testimony by dismissing dramatic scenarios of cyber Armageddon. It may be worth mentioned a few other scenarios that are worth dismissing. We often hear that the Federal government should lead by example and secure its own networks before advising the private sector. This is a recipe for disaster. The Federal responsibility is to provide for the defense of

the entire nation. We sometimes hear that the market will provide the innovations we need for security. I myself wrote this in 1996 and I have been waiting 13 years for those innovations – we need to admit that the market will not deliver without incentives an intervention from the government. Sometimes we hear that since the private sector owns and operates most infrastructure, they should lead in securing cyberspace against foreign militaries and intelligence services or highly skilled international criminals, but this is like saying that America's airlines should secure our airspace against foreign air forces An easy rule of thumb is that any argument that was used to undercut the 2003 National Strategy – and all of these arguments were used then - should be discarded in the current debate. We chose weakness in 2003 and have paid for it ever since.

The United States has made better use of cyberspace than our competitors, and this has provided real economic benefits. Our reliance on cyberspace holds the potential for recovery and future growth. We cannot turn away from cyberspace, nor can we afford to forgo the opportunities it will create. However, the combination of greater reliance on cyberspace and inadequate attention to security has left us more vulnerable than our opponents. If this is not changed, United States will see the continued erosion of its power and influence and our prosperity and security will be irrevocably damaged. Congress and the executive branch have the opportunity to avert this outcome if they act decisively and promptly.

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