House Committee on Homeland Security
Subcommittee on Cybersecurity, Infrastructure protection and Security Technologies
"Examining the Cyber Threat to Critical Infrastructure and the American Economy"
March 16, 2011
Testimony of James A. Lewis
Center for Strategic and International Studies

Chairman Lungren, Ranking Member Clarke, and Members of the Committee. Let me begin by thanking you for this opportunity to testify on this important subject.

Cybersecurity first came to the attention of the public in the mid 1990s, some fifteen years ago. The first major policy for cybersecurity, Presidential Decision Directive 63, appeared in 1998. In the intervening years, there has been much discussion and a few new ideas. We can get a sense of the state of cybersecurity and whether there has been any progress the U.S. by reviewing major cybersecurity events that have occurred since the start of 2010.

- **January 2010**: Google announced that an attack had penetrated its networks, along with the networks of more than 80 other US high-tech companies. The goal of the penetrations, which Google ascribed to China, were to collect technology, gain access to activist Gmail accounts and to Google's password management system.

- **January 2010**: Intel Corporation also disclosed that it has experienced a harmful cyber attack at the same time

- **January 2010 Global** financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same hackers who attacked Google, according to leaked e-mails.

- **March 2010**: NATO and the EU warned that the number of successful cyber attacks against their networks have increased significantly over the past 12 months.

- **March 2010.** Australian authorities say there were more than 200 attempts to hack into the networks of the legal defense team for executives from Australian energy company Rio Tinto, to gain inside information on the trial defense strategy.

- **April 2010**. Hackers break into classified systems at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian defense and armament planning.

- **May 2010.** A leaked memo from the Canadian Security and Intelligence Service (CSIS) says, "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially.... In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage."

- **October 2010:** Stuxnet, a complex piece of malware designed to interfere with Siemens

Industrial Control Systems discovered in Iran, Indonesia and elsewhere, results in significant physical damage to the Iranian nuclear program.

- **October 2010.** The Wall Street Journal reports that hackers using "Zeus" malware, available in cybercrime black markets for about $1200, were able to steal over $12 million from five banks in the US and UK.

- **December 2010** British Foreign Minister William Hague reported (in February 2011) attacks by a foreign power on the UK Foreign Ministry, a defence contractor and "other British interests." The attack succeeded by pretending to come from the White House.

- **January 2011.** The Canadian government reports a major cyber intrusion involving the Defence Research and Development Canada, a research agency for the Department of National Defence, the Department of Finance, and the Treasury Board, Canada's main economic agencies. The intrusions forced the Finance Department and the Treasury Board, to disconnect from the internet.

- **March 2011.** Hackers penetrate French government computer networks in search of sensitive information on upcoming G-20 meetings.

- **March 2011.** The Republic of Korea said that foreign hackers penetrated its defense networks in an attempt to steal information on the U.S.-made Global Hawk unmanned aircraft, provided to Korea as it considers whether to buy the UAV.

Major corporations, financial firms, government agencies, and allies have all been victims, and these are just the events we know about. There are of course many more incidents stretching back into the 1990s, that include the loss of tens of thousands of pages of sensitive military information, market and exploration data worth millions from oil companies, the loss of valuable commercial technologies, and hundreds of millions of dollars from banks and other financial institutions. Classified military networks have been penetrated by foreign intelligence agencies. Best of all, from the perpetrators' perspective, no one have ever been punished for any of these actions.

This is not a record of success. Whatever we are doing is not working. Since 1998, we have repeatedly tried a combination of information sharing, market based approaches, public private partnership and self-regulation in a vain effort to strengthen our cyber defenses. However, despite this dispiriting record of opponent success, I feel confident in predicting that this year, the old, failed formulas will be trotted out again this year. Many of the reports and essays we see emerging now will advocate tired ideas in order to block change rather than increase cybersecurity. While individual government agencies have made strenuous efforts to improve our cyber defenses, as a nation, despite all the talk, we are still not serious about cybersecurity.

This is due to a reluctance to make the changes cybersecurity requires. People still advocate strategies and policies that appeared more than a decade ago and which have not worked. We have consistently underestimated the risks and damage from weak cybersecurity. Everyone is for better security, but there has always been some other objective that seemed more important.

Cybersecurity is another of those situations in American history, ranging from Pearl Harbor to 9/11, where we knew there was risk and that we were unprepared, but assumed it would never happen because America is too powerful or too big to attack.

Nothing has yet punctured this misplaced sense of invulnerability. America is still powerful, and it is easy to say that the sky is not falling and there is no need for haste. The effect of this over confidence is to make tolerable the slow erosion of our national power due to feeble cybersecurity. Some call it the 'death of a thousand cuts," where each tiny cut goes unnoticed by the victim. There are warning signs that even a nation as rich and as powerful as the U.S. is at risk. The challenges to our financial system and the loss of manufacturing and innovative capabilities are subjects for another hearing, but weak cybersecurity exacerbates these problems. Business as usual means long-term decline as our economic and technological leadership is damaged by cyber espionage.

There are also two sets of risk. One is immediate and real. Two of our potential military opponents have the capability to launch damaging cyber attacks against America's critical infrastructure. The Aurora test at the Idaho National Labs and the Stuxnet worm showed that cyber attacks can do physical damage. These opponents have carried out network reconnaissance against critical infrastructure to allow them to plan their attacks. The issue for this committee is that after twelve years of information sharing, public private partnership, and voluntary action, critical infrastructure in the U.S. is not ready for an attack.

While these militaries have the capability to launch a damaging cyber attack, they are unlikely to do so short of an armed conflict. They are deterred by the threat of an American military response. Only if we were to get into a shooting war with them, over Taiwan or Estonia, could we expect to see cyber attacks. However, while we can deter military attack, our military strength does not deter espionage and crime in cyberspace. Deterrence not a solution for cybersecurity's most pressing problems.

Cyber terrorism is still a distant threat, but it is a threat that is increasing. Terrorists lack the capability to launch cyber attacks. If they had this capability, they would have already used it. Our original emphasis on "cyber terrorism" was wrong. The day a terrorist group gets cyber attack capabilities, they will use them. At that moment, if we have not improved our cyber defenses, they will succeed in causing disruption and damage. It is concerning to note that a few terrorist groups have expressed interest in acquiring cyber attack capabilities – the most recent was Al Qaida in the Arabian Peninsula (AQAP). This group is worrisome. They are inventive in using the internet for propaganda and organization, and they have said one of their goals is to disrupt the American economy – this was the alleged motive for their effort using printer cartridges in air shipments. We have some number of years – I hope – before AQAP or another group, or an irresponsible nation like North Korea or Iran, acquires cyber attack capabilities, because we will not be able to deter them from attacking and our defenses are inadequate.

If there is one conclusion that we can draw from the long list of cyber incidents, it is that we are not prepared to defend ourselves. So we are vulnerable, but the risk of attack is low for the moment. As long as our opponents do not attack us, we are safe. This is not an ideal strategy for a superpower. Our current approach to cyber security leaves initiative and control to our

opponents. It also is ineffective in stopping the slow but steady damage to our economy and to our national security that comes from cyber espionage.

Remedying the situation will take a concerted effort, but we are far from consensus on how to proceed. We will hear that public-private partnership is essential, because the private sector owns 85% of critical infrastructure. The private sector owns 100% of the airlines in the U.S. as well, but no one uses this as an excuse to say we do not need an air force. We will hear that the internet must be protected because it is a source of innovation. Now, in other fora, it is common to hear that the U.S. is lagging behind in innovation, so it is fair to ask just how much the internet has helped. Innovation is a complex process and focusing on the internet as its source is probably wrong, perhaps a last left-over form the dot com bubble. But the notion that ability to better protect intellectual property and proprietary business information will somehow hurt innovation is bound to reappear. We will hear that technology moves to fast for regulation, but this is true only if you try to write prescriptive regulations. It is an avoidable mistake. And there will be a call for incentives, as if paying for an inadequate defense will somehow make it better.

No sector has a greater incentive than banks to protect their networks. They are a constant target. Some banks, particularly the top tier banks, have sophisticated defenses. Despite this, they are hacked. This is not surprising considering the thousand of probes they face each year, but even with all the incentives in the world and with a strong focus on cybersecurity that is matched in few other critical sectors, they cannot be secure. If the banks cannot protect themselves, why do we think other sectors will be able to do so?

The business implications for spending on cyber security by private companies, especially critical infrastructure companies, are straightforward. Investing in increased cybersecurity requires them to spend on nonproductive assets. They will not get an increased return on investment from this spending. There is a notion that if we could only demonstrate the scope of the losses, companies would be incentivized to recalculate the business case for cyber security and spend more. This may not make sense for critical infrastructure. The bulk of the losses come from the theft of intellectual property from commercial research and manufacturing companies. Critical infrastructure companies are likely experience less loss of this kind of data. The risk they face is the potential for service disruption, but before the disruption occurs, the cost may be so low as to be unnoticeable.

Additionally, it is likely that some industry sectors are more important than others for cybersecurity. Opponents may consider the defense, high tech or energy sectors as higher value targets for economic espionage. Electrical and telephone grids may be high value targets for critical infrastructure attacks, as disrupting them could have cascading effects through the economy. The financial sector may be particularly attractive as it is both a critical infrastructure – stop the flow of money and you trigger immense disruption- and attractive as a target for crime. There are indications that the financial sector and the electrical grid face increasing risk because of heightened opponent interest (whether state or criminal) in these sectors as targets.

This has implications for a national resiliency strategy. Without external incentives, companies will be unwilling to invest in redundant infrastructure to provide resilience. On the other hand, providing incentives without also being able to enforce compliance means at best, we will get a

very uneven level of implementation and continued vulnerability. Incentives only make sense if increased authority for the Department of Homeland Security (DHS) accompanies them. Incentives by themselves are a give-away without benefit to security.

Incentives will not solve the problem of our reliance on a disaggregated, point cyber defense, where each network or user is responsible for their own defense. This is the worst possible defense against a skilled opponent. Every company is on its own, and they can be picked off one by one. Providing incentives without being able to coordinate our cyber defenses and ensure a common level of performance it not an improvement.

Voluntary action is also not enough. Is there a more sophisticated technology company than Google? Google has unparalleled skills and resources. The same is true for Intel, Adobe, Microsoft, and the many other companies that have allegedly been hacked. Voluntary action by even the most sophisticated tech companies is inadequate. The reason for this is simple. Pros always beat amateurs. We are asking corporations to take on the most powerful military and intelligence agencies in the world, agencies that do not observe our laws and that do not like us. It is no contest. It is like sending the company softball team against the Giants or the Yankees. Voluntary action by itself will always be inadequate against dangerous foreign opponents.

Efforts to secure the Smart Grid are a good example of the problems with a voluntary approach. Security standards published by the National Institute for Standards and Technology in August 2010 were developed by a consensus process that included 475 participants from the private sector participants. A consensus process involving 475 people is itself problematic. This is why the founders wisely opted for majority rule in the Constitution. A report by the General Accountability Office from January 2011 found that since these consensus standards are voluntary, there is no way to enforce them or even know if companies are following them. Perhaps unsurprisingly, the GAO also found that critical smart grid elements "do not have adequate security built in, thus increasing their vulnerability to attack."[1]

Voluntary action has not worked, but some argue it deserves another chance and that we should pay companies to put better cybersecurity in place, using incentives, but that we should also not tell them what to do. This is a recipe for disaster. There is no other area of national security were we rely on voluntary action reinforced by incentives. A policy of voluntary efforts for better cybersecurity reinforced by incentives is not a serious effort to protect national security against real damage and a growing threat. These proposals are best seen as intended to block reform rather than to promote cybersecurity.

Information sharing is a more difficult problem. No single agency or company knows the full range of threats we face in cyberspace. The National Security Agency, cyber Command, and DHS have part of the puzzle, the big telecom companies have another part, the antivirus companies and big internet service providers another. If we could put these parts together, our ability to protect the nation would be significantly improved. Perhaps twenty or thirty companies and two or three agencies would need to share information and be partners in a national defense. This would be a public private partnership that could make a difference.

[1] GAO, Electricity Grid Modernization (http://www.gao.gov/new.items/d11117.pdf)

And of course, it is impossible do to this in the U.S. Our laws and our policies block the one area where we could have meaningful public private partnership and information sharing that could make a difference. Some of the very organizations that stoutly proclaim the need for public private partnership also object to meaningful information sharing, the one area where public private partnership makes sense.

After 12 years of experience, we can now say with confidence that a voluntary approach to cybersecurity based on public private partnership and information sharing is inadequate to defend America. These are elements of a comprehensive defense, but by themselves they are not enough. They must be reinforced by an active defense that uses our military and intelligence assets, by flexible regulation of critical infrastructures and internet service providers, by a strong diplomatic effort to extend the rule of law into cyberspace, and by expanding law enforcement cooperation in every country to which we are connected.

In December 2008, CSIS issued a report by its Commission on Cybersecurity for the 44th Presidency that laid out a number of recommendations for a comprehensive national approach to cybersecurity.[2] While the report was well received, the implementation of the recommendation has been slow. In February 2011, the Commission issued a second, final report[3] that assessed where progress still needs to be made. We identified ten key areas and listed the tangible steps that need to be taken. The most important of these were the need for coherent Federal leadership, clear authority to mandate better cybersecurity in critical infrastructure, and a foreign policy that used both military and diplomatic tools to bring the rule of law to cyberspace.

These are crucial areas for improvement, but each raises significant issues for the upcoming legislative debate. One issue is whether DHS or at the White House should lead cybersecurity efforts. In this case, there is not simple answer. DHS is best placed, working with the Department of Defense and the National Institute of Standards and Technology (NIST) , to develop standards and regulations. DHS is best placed to work with first party regulators – FERC, FCC, FFIEC and others – to ensure compliance. On the other hand, the White house is best placed to develop a national strategy, to coordinate military, intelligence, law enforcement and diplomatic activities, and to provide executive branch oversight and guidance for cybersecurity activities and for privacy protection.

The first CSIS report discussed a new, flexible approach to regulation that gave the private sector a greater role in designing the rules while leaving enforcement to the Federal government. Now, it is quite true that regulation done badly can be very damaging. There are countless example of that kind of prescriptive overregulation and finding ways to streamline regulation is an essential task for America. It is also true that no regulation leads to disaster. Even the strongest proponents of deregulation do not call for the elimination of the Federal Aviation Authority. All the airlines mean well and do their best, but we do not feel comfortable leaving air safety to voluntary action because lives are at stake. We do not feel comfortable saying to companies, you make the decision on whether to sell nuclear or missile technology to a foreign customer. We regulate them. Public safety and national security require it. Regulation is unpleasant, but in some cases, the alternative is worse. Cybersecurity is one such case. The approach proposed in

[2] http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf
[3] http://csis.org/files/publication/110128_Lewis_CybersecurityTwoYearsLater_Web.pdf

draft legislation, which is based on the Chemical Facilities Anti-Terrorism Standards found in the Homeland Security Act, offers a reasonable approach to better cybersecurity.

Precedents for a new approach can be found in recent changes to the implementation of the Federal Information Systems Management Act Reporting Guidelines or in the Consensus Audit Guidelines developed by a consortium of federal agencies including NSA and private organizations. These guidelines identify technical security controls that are effective in blocking high-priority attacks. They show that is possible to identify practices that improve cybersecurity and measure their effectiveness, since technology does not change too fast. I recently spoke to the Deputy Chief Information Officer of an agency that had implemented the guidelines - this was an agency that suffered major losses to hacking a few years ago – and he said the improvement in their defenses has been dramatic. I asked if the Guidelines are not getting out of date, as they are two years old, and he replied that not only are they are still effective, that implementing the first four guidelines stops most of the attacks. It is now possible to identify effective practices and continuously measure how well they work – if they are implemented.

A comprehensive strategy that coordinates military, intelligence, law enforcement and diplomatic activities is essential for securing a global network. Reducing cyber crime will require a strategic, national-level approach that uses law enforcement, intelligence and diplomacy. The most sophisticated cyber criminals live overseas, in countries that do not cooperate with U.S. law enforcement. The problem is complicated by the fact that a few countries tolerate and even encourage cyber criminals. They use them as proxies, as irregular forces to carry out operations for the government. The provide resources and sometimes training. It will not be an easy task to get these countries to stop cybercrime, and there is little that the private sector can do.

Limitations on the use of our military and intelligence capabilities continue to weaken cybersecurity in the United States. A case from last year shows the situation. We are told that a leading American bank had its networks penetrated by Russian hackers. The hackers extracted millions of dollars. The bank, of course, said nothing publicly. But while the crime was in progress, it was detected by an American intelligence agency. As an intelligence agency with no domestic authority, there was nothing it could do other than relay the information to law enforcement agencies, a cumbersome process under today's laws. By the time this was done, the crime was over. Active defense would have let the intelligence agency detect the incoming attack on the internet backbone, on the borders of America's national networks, and stop it. Active defense could be structured to operate like NORAD, where the Air Force protects our skies, by focusing on foreign threats. It is not perfect, but it works and other nations are deploying this kind of defense against foreign attacks.

Active defense is the future of cybersecurity. It raises two key issues, the first being the need for additional privacy safeguards and oversight and the second being the division of responsibility between DHS and DOD. Stronger cybersecurity probably requires a new approach to privacy and a strengthening of existing oversight mechanisms. To give two examples, the Privacy and 'Civil Liberties Oversight Board, PCLOB, does not have cybersecurity in its legislative charter, nor is there executive branch guidance (along the lines of Executive Order 12333, which governs intelligence activities) for agencies in how to perform their cybersecurity missions. Both of

these reflect the need to adjust our laws and regulations to the new cyber environment.

DHS and DOD both have important and potentially complementary roles to play in cybersecurity. DHS is best placed to work with critical infrastructure and to ensure domestic preparedness. Only DOD has the capability to respond to foreign opponents. There are still coordination issues that need to be worked through, and some of these issues will be resolved only when the White House has a stronger role in cybersecurity, but the recently signed Memorandum of Understanding signed between Secretaries Napolitano and Gates is an important first step in building a coordinated defense.

The problem of international engagement is challenging, in part because for years the U.S. believed that cyberspace would be some kind of self-governing utopia. As the security situation worsened, as cyberspace became a new domain for conflict, and as the political implications of the new technologies became apparent, other nations have decided to extend government control into cyberspace. This trend is irreversible. The U.S. must engage with these nations in order to influence, if not lead, this restructuring of cyberspace governance, in order to ensure that the political values we cherish – openness, global connectivity, and freedom of speech – continue to guide development of the global network. Thinking on how to do this is at a very early stage. New kinds of expertise are required and there are only a handful of people with relevant experience. The State Department has just created a new cyber coordinator position and with the right support form Congress, this could allow the U.S. to regain international influence.

These are complicated issues and the account above is necessarily summary. They receive more detailed treatment in the CSIS reports. However, in drafting the final report, we found that as the prospect for change increases, so will resistance to it. People are wedded to old ideas, even if they do not work. New kinds of expertise are required for understanding cybersecurity. Above all, many still place some other priority above securing our nations networks.

It is this last point that worries me the most. When we look at nations that have fallen on hard times, losing their power and their international standing, very often it was because of internal problems. Often, the leaders of these countries knew what the problems were. They even knew what the solutions were, but their beliefs and reliance on old approaches kept them from making the needed changes. So far, this has been the case with cybersecurity in America. We are in a new world and face new problems that old ideas will not solve, but it is hard to give them up. Better cybersecurity is possible, but not if we continue to use failed approaches.

This puts a great responsibility on Congress and the White House. We have a real opportunity in the next two years to improve our cyber defense. Doing this will require leaving old ideas behind, even though many will still advocate them, and moving to a new, comprehensive approach to cybersecurity that treats it as a major component of national defense and homeland security. I thank the Committee for the opportunity to testify and will be happy to take any questions.