"Cybersecurity: Next Steps to Protect Critical Infrastructure."
February 23, 2010
Senate Commerce Committee
James A. Lewis, Center for Strategic and International Studies

I would like to thank the Committee for this opportunity to testify and I would like to congratulate it for its comprehensive "Cybersecurity Act of 2009."
This bill is important because it is a broad step to rethinking our approach to the internet, to cyberspace, and to the role of government.

The pioneers of cyberspace wanted governments to have a very limited role. They expected a self-governing global commons to emerge, and argued that there were no borders, that technology moved to fast, that old rules of business and security did not apply. They expected a global commons; instead they got the wild west. The internet was not designed to be secure; the rules and contracts put in place when it was commercialized were not written with security in mind. The result is Hobbesian, that is to say nasty and brutish, if not short. So the issue for the nation is how to bring law to the Wild West, how to move from a do-it-yourself homebrew approach to cybersecurity, and how to secure a global digital infrastructure upon which we now depend. Legislation like the Cybersecurity Act 0f 2010 can play a crucial role

Cybersecurity has become an important issue over the last decade as the internet changed to become a significant global infrastructure. The U.S. in particular has woven computer networks into so many of its economic activities that we are as reliant on the internet as we are on any other critical infrastructure. Networked activities can be cheaper and more efficient, so companies large and small have migrated to the internet because it can provide competitive advantage. Our national defense relies heavily upon networks. Networks reinforced existing trends in military the realization that intangible factors – greater knowledge, faster decision making increased certainty – would increase effectiveness of our military force.

That technologies designed in the early 1970s have worked so well and have so cleanly scaled to support more than a billion users is an amazing triumph, but anyone with malicious intent can easily exploit these networks. The internet was not designed to be a global infrastructure upon which hundreds of millions of people would depend. It was never designed to be secure. The early architects and thinkers of cyberspace in the first flush of commercialization downplayed the role of government. The vision was that cyberspace would be a global commons led and shaped by private action, where a self-organizing community could invent and create. This ideology of a self-organizing global commons has shaped internet policy and cybersecurity, but we must now recognize that this pioneer approach is now inadequate.

There are two reasons for this inadequacy. First, private efforts to secure networks will be always be overwhelmed by professional military and criminal action. The private sector does not have the capability to defeat an advanced opponent like the SRV or the PLA, organizations that invest hundreds of millions of dollars and employ thousands of people to defeat any defense. We do not expect airlines to defend our airspace against enemy fighter planes and we should not expect private companies to defend cyberspace against foreign governments.

Second, absent government intervention, security may be unachievable. Two ideas borrowed from economics help explain this - public goods and market failure. Public goods are those that benefit all of society but whose returns are difficult for any individual to capture. Basic research is one public good that the market would not adequately supply if government did not create incentives. Cybersecurity is another such public good where market forces are inadequate.

We talk about cyber attack and cyber war when we really should be saying cyber espionage and cybercrime. Espionage and crime are not acts of war. They are, however, daily occurrences on the internet, with the U.S. being the chief victim, and they have become a major source of harm to national security. The greatest damage to the U.S. comes from espionage, including economic espionage. We have lost more as a nation to espionage than at any time since the 1940s. The damage is usually not visible, but of course, the whole purpose of espionage is not to be detected.

This is not cyberwar, Russia, China, and cybercriminals of all types have no interest in disrupting Wall Street, the internet, or the American economy. There is too much to steal, so why would anyone close off this gold mine. As with any good espionage exploit or mafia racket, the perpetrators want stability, a low profile, and smooth operations going so they can continue to reap the benefits.

There is a potential for cyber attack, but it is so far constrained by political and technological barriers. Terrorists likely do not yet have the advanced cyber capabilities needed to launch crippling strikes. The alternative, that they have these capabilities but have chosen for some reason not to use them, is ridiculous. There are nations that could launch a crippling strike, but they are likely to do son only as part of a larger armed conflict with the United States. These nations do not love jihadis any more than we do, so they are unlikely in the near future to transfer advanced cyber capabilities to terrorists. Presumably, in the case of Russia and China their cyber criminal proxies are also instructed not to take jihadi clients (although there is one incident where it is alleged that Russian hackers served as mercenaries for Hezbollah, against Israel). Should any of these conditions change – the technological constraints that limit terrorists and the political constraints that limit states and advanced cyber criminals - the U.S. is in no position to defend itself against cyber attack.

Short of armed conflict (over Taiwan or Georgia), China or Russia are unlikely to use cyber strikes against the U.S. The political risk is too high – it would be like sending a bomber or a missile against a power plant, and the U.S. response would be vigorous. Our opponents, however, have reportedly conducted reconnaissance missions against critical infrastructure – the electrical grid, for example – to allow them to strike if necessary in the event of conflict. Cyber attack is cheaper and faster than a missile or plane, there is some chance that the attacker can deny responsibility (because of the weak authentication on the internet). Right now, our opponents have the advantage but it is within our capabilities to change this.

Getting this change requires a new approach. Many of the solutions to the problem of cybersecurity our nation has tried are well past their sell-by date. Public-private partnerships, information sharing, government-lead-by-example, self-regulation, and market-based solutions are remedies we have try for more than a decade without success. These policies overestimate incentives for private action and misalign government and private sector responsibilities.

Like other new technologies in the past – airplanes, cars, steam engines – the appeal and the benefits are so great that we have rushed to adopt the internet despite serious safety problems. These problems are amplified by the global connectivity of the new infrastructure, as the speed of internet connections means that geographical distance provides little in the way of protection. For those earlier technologies, safety came about through innovation driven by government mandates, and by agreements among nations. The same process of development is necessary to secure cyberspace. The Cybersecurity Act of 2009 could play a vital role in this improvement.

This will not be an easy task. The United States does not like to deal with market failure. This has been true since the earliest days of the republic. Steam engines, although notoriously unsafe, had to wait forty years until a series of savage accidents costing hundreds of live led Congress to impose safety regulations. Automobile safety rules took more than half a century and initially faced strong opposition from manufacturers. The initial air safety regulations appeared only twenty-three years after the first flight. There is the recurring hope that "intellect and practical science," to quote a 19th Century Congressional report explaining why regulation was unnecessary for steamboats put it, will lead to improvement via some automatic and self-correcting market process and without government intervention.

Just as cars were not built to be safe until government pressure changed auto manufacturers' behavior, cyberspace will not be secure until government forces improvement. Twelve years of reliance on voluntary efforts and self-regulation have put us in an untenable situation. Some may argue that a move away from the market or a greater emphasis on security or a larger role for government will damage innovation in cyberspace. This argument is in part a reflection of competition among various bureaucracies, advanced to protect turf, but is also reflects a misunderstanding of the nature of innovation. There are grounds to be concerned about the ability of the U.S. to innovate when compared to other nations, but the real obstacles are a weak education system, poorly designed tax policies, damaging immigration rules, and mis-investment that makes it hard to develop new technologies and competitors. Removing these obstacles would be politically difficult and face strong opposition. It is easier to insist instead that keeping the internet open and anonymous or bringing broadband to undeserving areas will somehow generate growth. Greater security is more likely to increase innovation, by reducing the loss of intellectual property and by increasing demand for more valuable internet services

Another reason put forward for not taking action is the supposedly borderless nature of cyberspace. The pioneers of cyberspace wanted their new creation to be a global commons, a shared space that no one owns. The designers of the internet built the network to reflect their values, which were non-hierarchical and to a degree, antiauthoritarian and anti-government. One of the original cyberspace theorists was also a songwriter for the Grateful Dead, and it was he who issued the famous Declaration of Independence of cyberspace, saying there was no room or need for governments. Cyberspace would be a global commons where a self-organizing community could invent and create.

This is an ill-conceived notion that continues to distort our thinking. Cyberspace is an artificial construct produced by machines. Those machines are all owned by individuals or organizations and all exist in some physical location that is subject to the sovereign control of some nation.

Cyberspace is like the public space in a shopping mall, a “pseudo commons” or a condominium.

In some instances, of course, such as the Internet Engineering Task Force or the Open Source Software Movement, this vision of an open, nonhierarchical community has worked exceptionally well. But to use a historical analogy, many of the pioneers of the internet expected Woodstock and the “Summer of Love,” instead they got Altamont and the Hells Angels. The combination of unplanned global access, porous technologies, and weak governance makes this newly critical infrastructure exceptionally vulnerable. As our reliance as a nation increases, so does our vulnerability to remote exploitation and perhaps attack.

Cyberspace is not a global commons. It is a shared global infrastructure. There is rarely a moment when a collection of bits moving from one computer to another is not actually on a network that someone owns and that is physically located in a sovereign state. The exceptions might be undersea cables or satellite transmissions, but the action still takes place on an owned facility were the owner is subject to some country and its laws. At best, this could is a "pseudo commons." It looks like a commons but actually is not, as someone owns the resources in question and that someone is subject to the laws of some nation. Cyberspace is in fact a more like a condominium, where there are many contiguous owners

Governance of this condominium is both weak and fragmented. There are no agreed rules, other than business contracts, and no “condominium board,” no process to develop rules. Action in cyberspace takes place in a context defined by commercial law and business contracts. When the United States commercialized the internet, it chose this legal construct accommodate business activity, but it is inadequate for security, particularly as the Internet spread to countries around the world and to nations with very different values and laws.

The proposed legislation would go a long way to correct these problems. To put the problem in a larger perspective, it is time to move from the policies created in the pioneer phase of the internet. It is time to close the Wild West. This will require a broad rethinking of American law and policy, and will require adapting to the technologies we now depend on. It will need new kinds of international agreements, new standards and rules for industry, and new approaches to the professionalization of those who operate networks. This is no small task but, judging from experience, it is inevitable. This process has occurred before, often with help from the government. The Commerce Department of the 1920s, for example, encouraged several major industries, including the automotive and radio industries, to standardize, to professionalize, and to create associations and rules that serve the public interest.

A “one size fits all” strategy will not work. We will need to manage international engagement, critical infrastructure regulation, and economic stability all at the same time. Progress faces significant obstacles. There are legitimate concerns over civil liberties. There are strong business interests in avoiding regulation. And there are the tattered remnants of a vision of cyberspace as some kind of utopian frontier. Governance is a central issue for each of these. Governance is the process for creating rules, resolving disputes, and ensuring compliance. Our beliefs about the nature of cyberspace have downplayed the role of formal governance and now we are paying the price. Changing this, as we did for steamboats, cars and airplanes, is part of the long-term process to adjust to new environment created by technological change.

This bill contains many of the essential elements of the new approach we need. A comprehensive national strategy that considers all aspects of national security and puts forward along term vision for cyberspace is an essential starting point for making this new infrastructure secure. It will be essential, of course, to avoid merely repeating the formulas of 1998 or 2003 in a new strategy. We've heard repeatedly that there is a shortfall of individuals with the requisite skills for cybersecurity. The scholarships, competitions and workforce plans outlined in this bill would go a long way to repair this. The legal review and the intelligence assessment are long overdue. The call for the creations of a response and restoration developed with the private sector that the president could implement in a crisis is crucial for national defense.

As with any major piece of legislation, there will be considerable criticism. Some of this criticism is ideological, some reflects self-interest, and some is the result of a healthy skepticism as to our ability to carry out some of the ambitious measures contained in the bill. There was initially concern that emphasizing the authorities the President already has to intervene in network operations during a crisis would somehow give the ability to shut off the internet. This stemmed mainly from an inaccurate reading of the bill and perhaps from the desire to preserve the notion of cyberspace as an untrammeled commons where government has little or no role. Frankly, efforts to deny the President adequate authority in a crisis are like expressing a preference for Katrina-like disaster management. I hope we can do better.

No one ever disagrees with the notion of more education, but the more contentious aspect of the workforce development is the requirement for certification and training. Being able to certify that someone has the necessary skill and knowledge is a requisite part of professionalization. We do this for doctors, lawyers, pilots, barbers, plumbers and real estate agents. Some certification requirements are Federal, many are developed by states. Many in the IT industry believe that they are not ready for this step. Certification requires knowing what is useful and necessary and being able teach it and test it. It is on the former that there is disagreement – that we do not know what is necessary for security.

This may have been true at one time but I believe it is changing. In the last few years, as people have been able to collect more data on security problems, to develop metrics, and to identify steps will reduce risk, it is possible to think of a training program for cybersecurity. This is part of a larger move from compliance drive security, which has largely failed, to performance driven security. The concept of a cybersecurity dashboard found in Section 203 reflects this shift to a data driven approach to cybersecurity. The Act, if passed, will accelerate the development and professionalization of those parts of cyberspace that provide critical services to the nation.

These are all politically difficult issues, but this situation is not new. Every time a new technology has reshaped business, warfare and society, there has been a lag in developing the rules – law, judicial precedents, regulations – needed to safeguard society. Cyberspace is different in its global scope and in the immediate nature of the damage America suffers. Waiting for some natural process or perfect solution not only puts our nation at risk, it gives our opponents an advantage. We would be well served if Congress passed this bill.