House of Representatives Committee on Oversight and Government Reform
Subcommittee on National Security, Homeland Defense and Foreign Operations
"Cybersecurity: Assessing the Immediate Threat to the United States"
James A. Lewis, Center for Strategic and International Studies
May 25, 2011

No one expected the internet to become a critical global infrastructure, least of all the people who designed and built it. So we should not be surprised that it is not very secure and that it is easy for malicious actors to exploit. There is an asymmetry between our considerable dependence on the new technology and our ability to secure it – the internet is incredibly valuable but it is easy to attack. This asymmetry gives potential attackers an advantage that they have not been slow to seize. The result has been to create two broad categories of threats to American security, or for that matter, the security of any nation that uses the internet.

The first set of threats arises from the potential for cyberspace as a new avenue of attack for military purposes. The second threat arises from the ongoing use of cyberspace for crime and espionage, including economic espionage. The distinction between these two threats revolves around whether a malicious action in cyberspace is equivalent to the use of force, to an attack using conventional weapons. We tend to call everything bad that happens in cyberspace an attack, but it is more realistic to say that if there is no damage, death or destruction, it is not an attack. We know of only three cyber incidents that rise to this level – the Stuxnet attack, the reported blackout in Brazil, and the interference with air defenses in the Israeli raid on a Syrian nuclear facility. Everything else qualifies as crime or espionage.

Cyber warfare will involve disruption of crucial network services and data, damage to critical infrastructure, and the creation of uncertainty and doubt among opposing leaders. The Russian use of cyber exploits during their clash with Georgia suggests how cyber attacks might be used – to complement conventional forces rather than to replace them. The air raid against the Syrian nuclear facility is a good example of this. While jets streaked across Syria, air defense radars showed an empty sky. This "informational" aspect of cyberwar, where an opponent might scramble or erase data, or put in false information to mislead an opponent, is a new and forceful aspect of military conflict.

Most people know about the Stuxnet worm, when a cyber attack destroyed equipment at an Iranian nuclear facility. Stuxnet confirmed what a test at the Idaho National Labs in 2007 had already shown – that an attacker could remotely interfere with the software controlling critical infrastructure and damage or destroy machinery and equipment. This kind of "military grade" cyber attack is best seen as a new capability for long range, very rapid strikes against critical infrastructure, information and networks. Cyber attacks are faster than a missile and have a global reach, but their payload is much less destructive. This military aspect of the cyber problem is like other military threats to U.S. security, deterred in part by our capability for response.

At this time, only a few nations with advanced military or intelligence agencies have the ability to launch Stuxnet-like cyber attacks that could disrupt critical infrastructure. There are perhaps five or six such nations. Our most advanced cyber opponents have carried out network

reconnaissance against America's critical infrastructure. None of the countries with advanced cyber attack capabilities are likely to use them frivolously against the United States, but they are certain to use cyber attacks if we enter into a military conflict with them.

There is, of course, the possibility of miscalculation, if one of our opponents in cyberspace carries out an experiment or weapons test that goes out of control, or a reconnaissance effort that accidently disrupts critical services. This sort of miscalculation or error could result in events escalating from a single incident to a more damaging conflict, which is one reason why many nations worry about cyber warfare.

Our research suggests that thirty-six countries have military doctrine for cyber conflict. Very few admit to offensive capabilities, but it is reasonable to assume that many have, as part of developing defensive capabilities, at least considered offensive use. Cyber attack will be like the airplane – within a few years, no self respecting military will be without this capability. Cyber attack capabilities are easier to acquire than airplanes, and to quote the head of Israeli military intelligence, "cyberspace grants small countries and individuals a power that was heretofore the preserve of great states."

As cyber attack capabilities spread, our ability to prevent attacks will diminish. Confrontational states such as North Korea and Iran do not yet have the capability to launch cyber attacks, but both North Korea and Iran are making serious efforts to acquire cyber attack capabilities. It is inevitable that they will succeed, which is one reason why it is important for the United States to strengthen its defenses as soon as possible. The most sophisticated cybercriminals, who sometimes act as irregular forces for their host governments - could launch damaging cyberattacks, but their interest is in making money or carrying out espionage activities. This could easily change. We have not yet seen advanced cyber criminals act as attackers or as mercenaries, but this remains a possibility. The future will be the “commoditization” of advanced attack techniques that will enable a range of groups to consider cyber attack as an option.

Terrorists currently lack the capability to launch cyber attacks. If they had it, they would have already used it. The day a terrorist group can launch a cyber attack, it will do so. A few terrorist groups have expressed interest in acquiring cyber attack capabilities. They have said one of their goals is to disrupt the American economy – this was the alleged motive for the effort by al Qaeda in the Arabian Peninsula to tamper with printer cartridges sent via in air cargo. We have a few years before terrorist groups or irresponsible nations like Iran or North Korea become sufficiently advanced in their cyber attack capabilities to launch strikes against the United States.

However, most nations are afraid of unleashing cyberwar. They are possibly deterred by fear of a U.S. military response. They are careful, therefore, to stay below the threshold of what could be considered, under international law and practice, the use of force or an act of war. They concentrate their efforts on espionage and crime which, in cyberspace, carry almost no risk. There is little or no consequence for malicious cyber activities that do not involve the use of force. So while countries are very cautious in using cyber techniques for attack, they feel very little constraint in using cyber techniques for espionage or crime. Crime, even if state sponsored, does not justify a military response. Countries do not go to war over spying. For these reasons,

the immediate threat in cyberspace involves espionage and crime. These are daily occurrences.

Foreign competitors use cyber espionage to acquire our most advanced military technologies. One way to estimate the threat from cyber espionage is to look at the amount of material already lost. Sources at the State and Defense Departments say that by 2007, they had already lost perhaps six or seven terabytes of information. To put this in perspective, the 130 million books and manuscripts in the Library of Congress take up twenty terabytes. The loss of thousands of pages of documents and designs help explain many analysts say that the internet has created a "golden age" for espionage.

Foreign competitors use cyber espionage to steal business plans, intellectual property and product designs from companies. The effect is to undermine U.S. international competitiveness. While losses from piracy – the illegal copying of entertainment or software products - are significant, economic espionage poses the greatest threat. The U.S. spent $368 billion on research and development (R&D) in 2010, but cyber espionage lets other countries get the results for free. The December 2010 incident where Google and thirty other Fortune 500 companies were hacked and lost data, allegedly to a Chinese entity, illustrate the espionage problem. Google lost technology and its Gmail service was searched for information on Tibetan human rights activists. The technology acquired from Google and other American high tech companies will eventually improve Chinese products. The theft of intellectual property is a major trade issue that deserves greater attention and a real threat to America.

It is hard to estimate the losses from cyber espionage and cyber crime. Companies conceal their losses and some may not even be aware of what has been taken. Crime against banks and other financial institutions probably costs a few hundred million dollars every year. In contrast, the theft of intellectual property and business confidential information – economic espionage –cost developed economies much more. One estimate put U.S. losses of intellectual property and technology through cyber espionage at $240 billion. An estimate of German losses of intellectual property due to cyber espionage puts them at perhaps $20 billion. Since the U.S. GDP is roughly five times the size of Germany, a very simple extrapolation would put U.S. losses from intellectual property theft at $100 billion. These are very crude estimates, but they give some idea of the scope of the problem.

In the context of a $14 trillion economy, these losses appear small and perhaps this is why they do not attract much attention. Still it is baffling why a cyber- bank robbery that stole $11 million, such as occurred in the last year, attracted little attention. If gunmen walked into a local bank and stole a million dollars, it would be on every front page. Robberies of this size probably happen almost every month in cyberspace, yet they rarely attract notice. The theft of credit card data gets more attention. It remains a lucrative field for cyber criminals. A recent example – the theft of credit card data from the Play Station network - affected as many as 99 million people. Some say that so much was stolen that the price of credit card data in cybercrime black markets actually fell because of the glut.

These black markets support cybercrime. In the cyber black market you can buy the latest hacking tools, learn of recently discovered vulnerabilities, rent "botnets" (thousands of remotely controlled computers), or purchase personally identifiable information. Credit card numbers,

social security numbers, and bank accounts, can be bought in lots of five or ten thousand. Buyers can choose between 'raw' information or data that has been tested for accuracy. These black markets amplify the threat of cybercrime and help make it a professional activity.

There is increasing concern about the vulnerability of the American financial system to cyber disruption. How much of this concern is justified is difficult to say, but there are some disquieting signs. Last year's "flash crash," where automated trading systems briefly crashed the stock market shows the potential for cyber disruption. This year's penetration of NASDAQ, while it did not lead to any noticeable losses, shows the potential vulnerabilities of the system. While it is very unlikely that the nations with advanced cyber capabilities would crash the American financial system – they simply have too much invested in it – they could try to do so in the event of a war. It is more likely is that cybercriminals, in an attempt to manipulate stock prices or gain insider information, could inadvertently cause some kind of crash. Federal agencies, financial institutions and the major exchanges are all working to reduce the chances of this kind of damaging event, but it remains a possibility.

Malicious action against the information technology supply chain is another threat. Many nations, including both the U.S. and China, are worried about depending on a global supply chain for information technology products. Discussion of the supply chain problem is usually not very sophisticated. An astute opponent will not build in back doors into a product since these might be discovered. Better to sell a safe product with no errors that will pass inspection, and then exploit the knowledge and access from the sale to gain intelligence advantage and to increase the ability to disrupt infrastructure in a conflict. An obvious example of this would be for a company to sell a product that is completely secure and passes every test, and then to introduce vulnerabilities when they provide the inevitable "patch" to the software. How often do people examine a patch or update?

The growth of table computers and other mobile devices makes downloadable "apps" an interesting vehicle for malware delivery. When was the last time anyone thought about security when they downloaded an app? Apps are screened, of course, but usually to make sure they are interoperable. An astute opponent or criminal might offer an enticing game app for free and then reap the benefits.

Supply chain contamination is a real threat, but heavy-handed measures to reduce supply chain risk, such as intrusive product inspections by national agencies, will backfire. They will only reinforce the plans of other nations to use these techniques and harm American exports. WE need alternate approaches that will build trust. While there has been some useful progress in reducing supply chain risk, it may be impossible to eradicate it, and we may need to step back and ask how we can operate effectively on networks that, despite our best efforts, will have some degree of supply chain contamination.

A final category of cyber threat involves political action, although this may hold greater risk for countries other than the U.S. The European leftists behind the Wikileaks episode intended to damage the United States and to hurt its credibility and influence internationally. The effect was to help our opponents – jihadis and authoritarian regimes. We do not want to overstate the risk from events like Wikileaks, but those hostile to the United States will take advantage of poor

security of information and the global reach of the internet to damage the United States. There is also the threat that a foreign opponent might disrupt American elections. We know for example that campaign databases were hacked and information exfiltrated from both the McCain and Obama Presidential campaigns in 2008. While the data was apparently not used, it is easy to imagine someone leaking it to the media or taking other disruptive actions.

The most dangerous actors in cyberspace bear the unwieldy acronym APT, "advanced persistent threat." We have gone from high school students and "social hackers," who penetrated systems to gain prestige, to well-organized professional criminals and major intelligence agencies. Amateurs cannot defend themselves against these professional opponents – it would be like sending the company softball team against the New York Yankees.

Based on this survey, what can we say generally about threats to the U.S. in cyberspace? They are largely foreign, and foreign governments play a central role in directing or supporting them. They run the gamut from fairly simple fraud aimed at consumers to highly sophisticated espionage efforts. The best description would be that the greatest threats come from advanced, state-sponsored actors who have the skill and resources to overcome most defenses. The trend is that the less sophisticated threats will diminish, while the advanced threats will grow

This has serious implications for policy and helps to explain why so much of what we have done in cybersecurity has been ineffective. Reducing the threat to the United States requires a clear division of responsibility among agencies and between government and companies. But in the past, we have weighted this division too heavily in favor of the private sector. The threats we face come from increasingly professional sources, from intelligence agencies, militaries, state sponsored proxies, and from terrorist groups. No uncoordinated effort that relies on voluntary action will be sufficient to protect us against these threats. The private sector owns most of the shoreline, but we still need a navy. We do not ask airlines to defend our airspace against ballistic missiles, bombers, or fighter jets because they are incapable of defeating these foes. The same is true for cyberspace. We should ask companies to do only what makes sense from a business perspective and not ask them to should national defense burdens for which they are unequipped.

The most important function for a company is to make money, not provide for the national defense. National defense against professional opponents is a function only the Federal government can perform effectively. In some cases, meeting the challenge will require new partnerships – and we have seen successful partnerships in the financial and the defense industrial sectors. In other cases, it will require new incentives and federal authorities. An overview of threats and responsibilities suggests the following division of labor:

-- Innovation in new cybersecurity technologies is best left to the private sector. We would benefit across the board as a nation by removing regulatory and financial obstacles to the private sector's ability to innovate. Fundamental research, however, will require federal investment by institutions such as DARPA or the National Science Foundation. This was how the internet itself was created – the government funded the initial research, then passed it to the private sector for commercialization.

-- Supply chain threats are an area where the private sector is best equipped to understand

and respond to the problem. Some of the new partnership efforts created by the Departments of Defense and Homeland Security, and working with a small number of companies, have made real progress in securing the supply chain (although much work still remains).

-- Dealing with the threat of cybercrime requires close and equal partnership between companies and law enforcement agencies. FBI and Secret Service have worked closely and effectively with the financial community, for example, to pursue cybercriminals. The cybercrime threat can only be met through partnership, combined with strengthened cooperation with other governments.

-- Better information sharing would greatly improve our ability to understand and respond to cyber threats. If we could put together all the information held by cyber security vendors, internet and telecommunications service providers, and the intelligence community, we would have an almost complete picture of malicious activities in cyberspace. This will require new partnerships and new authorities. Government might need to be a partner and a participant rather than a leader. Neither private sector nor government have by themselves that complete picture. Companies complain that they get little useful information from government agencies. Some current laws, such as the 1986 Electronic Communications Privacy Act, may inadvertently hamper the ability to share information. Many of the groups created years ago to share information do not work and should be replaced. Information sharing is an area where partnership is vital, but we need to rethink our laws and find new approaches that serve the needs of both partners.

-- Bot-nets are an embarrassment for the United States. We are, inadvertently, one of the largest sources of cyber crime activity on the planet. Consumers do not know how to protect their computers and we are never going to be able to train them sufficiently. That means they are easy prey for cybercriminals, who seize control of their machines and use them for spam, denial of service attacks and other nefarious activities. Other nations, however, have developed an effective approach to bot-nets that is linked to information sharing. Consumers do not know when their computer has been captured but their service providers do. Making the service provider responsible for cleaning up bot-nets and malware on their costumer's computer would eliminate the problem. How do to this – whether through a voluntary consortia guided by government, as is the case in Australia and Germany, or in some other fashion, remains an open question. There is resistance from some service providers to taking on this responsibility for a variety of reasons, but both security and technology trends will eventually drive us to make service providers responsible for the security of consumer devices.

-- The threat to critical infrastructure also requires a close partnership between companies, the Department of Homeland Security and other regulatory agencies, but we can no longer rely on voluntary approaches or self-regulation in this partnership. We have used voluntary self-regulation for the last thirteen years and it is inadequate for national security. For example, although Stuxnet is the most dangerous cyber attack seen to date, a recent survey found that a third of the surveyed critical infrastructure companies did not even look for it on their networks. The new, more flexible approach to critical infrastructure protection that is modeled after the 109th Congress's Chemical Facilities Anti-Terrorism Standards, where industry develops the standards to meet potential threats and government makes sure they are adequate, offers a

solution that avoids prescriptive regulations without putting national security at risk.

-- The threat from foreign military and intelligence agencies can only be addressed by our own military, law enforcement, and intelligence agencies. No private company can match this class of foreign opponents, who can blend signals intelligence, human agents, and vast resources into an unstoppable package to penetrate networks, collect information, and if they wish, do damage. These opponents can bribe, steal, eavesdrop, spend millions to reverse engineer products, and work simultaneously in many countries around the globe. They draw in some cases on decades of experience in illegal activities and espionage. Defense, homeland security, and international law enforcement are federal responsibilities. We must approach these threats as we would approach any other threat to national security

We face a varied threat landscape in cyberspace. Countering these threats will require a balanced and comprehensive approach that to cybersecurity. This comprehensive approach is within our grasp if we can make a fresh start to addressing the problem. Yet when you talk to most people in the small community of cybersecurity experts, you will find a high degree of pessimism. Most of these experts believe that the U.S. will not adopt effective approaches to cybersecurity and will not move away from the ineffective policies of the past until we have some major incident, some disaster. I do not share this pessimism. The work of this committee and others will let us move ahead in making cyberspace more secure. I applaud the committee's work in calling attention to this and I thank you for the opportunity to testify. I will be happy to take any questions.

James Andrew Lewis

Director and Senior Fellow, Technology and Public Policy Program

Programs:

Authentication and Identification , Commission on Cybersecurity for the 44th Presidency, Cyber and Internet Policy, Cybersecurity Podcast Series , Cybersecurity Policy Series, Intellectual Property and Innovation, Intelligence Reform, National Security and Space, Technology and Public Policy Program

Topics:

Technology, Space, Cybersecurity, Technology Policy

James Andrew Lewis is a senior fellow and director of the Technology and Public Policy Program at CSIS, where he focuses on technology, national security, and the international economy. Before joining CSIS, he worked in the federal government as a foreign service officer and as a member of the senior executive service. His assignments involved Asian regional security, military intervention and insurgency, conventional arms negotiations, technology transfer, sanctions, Internet policy, and military space programs.

Lewis has authored numerous CSIS publications with the theme of how government policies adjust to technological innovation. They include *Building an Information Technology Industry in China: National Strategy, Global Markets* (2007); *Foreign Influence on Software: Risks and Recourse* (2007); *Waiting for Sputnik: Basic Research and Strategic Competition* (2006); *Globalization and National Security* (2004); *Spectrum Management for the 21st Century* (2003); *Assessing the Risk of Cyber Terrorism* (2002); and *Preserving America's Strength in Satellite Technology* (2001). Most recently, he was the project director for the CSIS Commission on Cybersecurity for the 44th Presidency, whose report has been downloaded more than 40,000 times. Lewis appears frequently in the press and serves on several federal advisory boards. His current research involves innovation and economic change, asymmetric warfare, and intelligence reform. He received his Ph.D. from the University of Chicago in 1984.

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: JAMES A. LEWIS

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2008. Include the source and amount of each grant or contract.

NONE

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

NONE

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2008, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

NONE

I certify that the above information is true and correct.
Signature: J A Lewis Date: 5/24/11