Testimony
Cybersecurity, Threats to Communications Networks, and Private-sector Responses.
House Committee on Energy and Commerce
Subcommittee on Communications and Technology
James A. Lewis, Center for Strategic and International Studies
February 8, 2012

Internet technologies are so desirable and so efficient that people proceed to use them without regard to risk. This means we are building vulnerability into the fabric of our economy. A disregard for risk has always been part of the adoption of new technologies, but past technology, risks were localized and not systemic: the internet is different. The behavior is the same, but the global scope, the incredible rapidity of connection, and inadequate technology changes the nature of risk and increases it.

Our vulnerability as a nation is increasing as our dependence on digital network technologies grows and as the skill and number of our opponents increases. Our cyber defenses have not kept up. This is largely a political problem. Our policies and our laws are inadequate. We now know how to reduce risk on networks, but we have chosen not to do so. From a planning perspective, it is best to start by assuming that no commercial or unclassified network is secure.

It would be easier to solve this problem if there was some big dramatic event – the Pearl Harbor everyone talks about – or if our opponents were foolish enough to start a cyber car. Neither of these is likely, however. There are of course countries with the ability to launch very damaging attacks – of the five or six countries with advanced cyber capabilities, two – Russia and China – bear us ill will and would use cyber attack in any conflict with the United States. But barring some miscalculation, they will avoid any action that could trigger an American response. They will stay below the threshold of the use of force that would justify an American military response. If they were to attack, however, we are defenseless because of our inability to move beyond antiquated notions of security.

The problem of lacking an adequate defense involves more that military conflict with Russia or China. Many other nations are acquiring cyber attack capabilities. The two most dangerous are Iran and North Korea. Anti-government groups, criminals and perhaps jihadis are also acquiring these capabilities. Two likely scenarios are worth considering, involving Iran and anarchic groups who may use the label "Anonymous."

Iran has been building its cyber attack capabilities for years. It is difficult from open source material to get a good picture of Iranian capabilities. The task is also complicated by ridiculous claims that come from Iran, such as the claim that Iran hacked into a U.S. drones. This is a nation, after all, that will routinely use "photo-shop" to make its missiles or other weapons look better. But just as Iran has doggedly pursued nuclear weapons, it has doggedly pursued cyber attack capabilities. Iran routinely probes Israel's networks to test its cyber capabilities. Iran was probably responsible for hacking the Dutch company "Digi-Notar" to acquire certificates that let them intercept communications for Iranian dissidents. Iran has close defense relations with China and Russia and may receive assistance in developing cyber capabilities. And Iran may feel that it is justified in launching a cyber attack since it was the victim of Stuxnet, the most

sophisticated cyber attack seen to date and which Iran blames on Israel and the U.S.

Director of National Intelligence James Clapper testified last week that Iran is losing its reluctance to strike domestic targets in eh U.S. It is easy to imagine the Iranian miscalculating, overestimating their ability to conceal their tracks, and launching a cyber attack. Perhaps they will use a proxy like Hezbollah or Hamas in an effort to conceal their involvement and to further complicate any American response.

Another likely source of attack in the future comes from the group "Anonymous." Calling "Anonymous" a group is something of a misnomer. Anyone can claim to be part of Anonymous. It can include teenagers with a grudge, the kind of anarchists who wear black masks and smash shop windows in violent protests, cyber criminals and perhaps even foreign intelligence agencies using the label as a convenient disguise. Anyone can engage in a malicious act and claim it "Anonymous."

This means it is very difficult to assess the range of cyber attack capabilities those who claim to be Anonymous may possess. Most of the actions attributed to Anonymous have been basic and Anonymous tends to exaggerate. But some in the hacker community say that some of the most skilled hackers in the world are among the ranks of Anonymous. We do have some idea of their motivations, which are anti-government and anti-American, and of their inventiveness, as they have been able to exploit corporate networks with ease.

If Iran or anarchists groups launched a cyber attack, what would it look like? It would likely not be catastrophic. Cyber "weapons" cannot cause mass casualties or mass destruction. Our own Department of Defense regards cyber as a "support weapon." A cyber attack will not be militarily decisive, but it will provide real advantage in any military conflict. Three recent incidents give us an idea of what a real cyber attack would look like.

Computer error caused the flash crash of 2010, when the stock prices temporarily collapsed. In this case it was inadvertent, but a moderately skilled attacker could be able to duplicate the effect. A more damaging attack might involve disruption and erasure of financial data. This kind of disruption of "Wall Street" would be attractive to some groups. Even selective targeting of a specific company or bank and its customers would cause an uproar. The 2003 Northeast blackout was also caused by inadvertent computer error. A moderately skilled attacker would also be able to duplicate this. It is possible to launch cyber attacks that are more damaging and which cause actual physical destruction, but these capabilities appear to be beyond what Iran or Anonymous could acquire in the near future.

Similarly, it is possible to interfere with other utilities. Anarchist might enjoy simultaneously turning all the traffic lights in the city green or having them change randomly. They could interfere with the water supply. Public utilities, financial services, communications – what we have come to call "critical infrastructure," are natural targets. They are routinely targeted by military planning and guerrilla operations. Before, insurgents might have pulled down power lines or blown up a substation. Soon, they will be able to use computers.

Of these, the electrical power supply is the most likely target. The cost-benefit ratio of attacking

this sector favors our opponents. Interrupting the flow of electrical power would be very disruptive, since we depend on electrical power, and it is the easiest to attack. Repeated studies have shown that control systems and critical networks are vulnerable and that companies may not even be aware of their vulnerability. In the future, when hackers want to protest bills like SOPA, they may turn off the lights in Washington instead of voluntarily blacking out a few websites.

The third predictive incident was the December 2008 penetration of DOD's classified network SIPRNET. This was carried out by a foreign intelligence service. No data was exfiltrated but the U.S. was unable, for a period of days, to remove the malware from SIPRNET. In a war, the foreign opponent could have used this malware to erase or scramble vital military data, disruption our command and control and greatly hampering U.S. operations. Of course, our most advanced opponents could also cripple critical infrastructure, but the first and perhaps only cyber attacks will be against military networks.

Incidents like SIPRNET or Stuxnet show that advanced attackers can penetrate any network. The crisis created by SIPRNET led DOD to take a number of steps to improve its defenses, including the creation of Cyber Command, imposing new requirements on defense contractors (whose networks are routinely targeted) and finding ways to share information with contractors and internet service provider. DOD recognized the scope of the problem and took steps to reduce risk. The same is true at other U.S. agencies that were the victim of cyber espionage. Others have not. There is little incentive to spend money to improve defenses

Other scenarios are of course possible. None of these incidents were catastrophic, and despite the weekly barrage of stories about cyber attacks and cyber war, most malicious activity in cyberspace involves either espionage or financial crime. Criminal acts are pretty straightforward – weak cybersecurity allows criminals to extract money. The best estimates suggest that this financial crime probably costs the U.S. several hundred million dollars a year. Most advanced cyber criminals live outside the U.S. or Western Europe, in countries that act as sanctuaries for cybercrime. Their activities are largely risk free, in that the chances of arrest or imprisonment are minuscule. They do this because cyber criminals form "proxy forces," irregulars whom the Government can call upon to carry out hostile cyber actions – this is what we saw in the politically coercive cyber activities aimed against Estonia and Georgia. Unwillingness to abandon these proxy forces explains much of the lack of progress in international cooperation against cybercrime.

There is a thriving black market in cybercrime tools and techniques and one issue to watch is how long it will take for advanced attack capabilities to appear for sale in these in these markets. Since there are links between governments with the most advanced cyber-attack capabilities and criminal proxies, we can expect that advanced capabilities will flow into private hands.

Espionage is directed against both government agencies and private companies. It is carried out by both intelligence agencies and private actors. American companies are prime targets. There is little public data on the full extent of their losses, since companies conceal when they have been hacked. But the U.S. has seen sensitive military technologies extracted by foreign opponents. Economic espionage against American companies is rampant, a symptom of the poor

network security prevalent in the U.S. and the lack of agreed international norms and penalties for malicious cyber activities.

Measuring the effect of economic espionage is difficult. Some cases are easy. When a foreign competitor steals confidential business information, such as oil exploration data or contract negotiations data, they get an immediate advantage that could be worth, in some instances, hundreds of millions of dollars. When they steal designs for advanced technology, as was the case in December 2010 when seventy U.S. high tech companies were hacked and lost data, it may take the opponents several to translate this data into actual products. But the long-term effect is to damage America's trade competitiveness and technological leaders, and to cost American jobs.

Fixing the problem of weak cybersecurity will not be easy. It will require a wide-ranging approach that works on an international, national, and individual level. The first element is greatly expanded international agreement between governments on their responsibilities in cyberspace. This will need to include common understandings on how international laws apply, including the laws of armed conflict, expanded law enforcement cooperation, better internet governance, and a stronger enforcement of trade rules, including penalties for failing to protect intellectual property.

Part of this will require developing and publicizing military doctrine and policies to warn potential attackers. A more difficult issue will require deciding what role the military and intelligence agencies will play in defending domestic networks. This is unavoidable because agencies like NSA are the most skilled and have the most knowledge about cyber defense, but our laws limit their involvement in domestic activities.

A strong national defense will involve improving cybersecurity in selected critical infrastructure sectors – power and energy, finance and telecommunication. Some of these sectors already do a good job and very little additional government action is required. Telecommunications companies have a business interest in providing reliable service to their customers. The same incentives do not exist in most other critical sectors, however, and government intervention will be necessary in those cases.

The first of these additional steps is to incentivize "enterprise" level defense by critical infrastructure companies. Critical infrastructure companies must be incentivized to provide adequate digital security, particularly for securing industrial control systems that control crucial machinery. The Stuxnet attack successfully targeted these control systems, and hackers can use the internet to remotely access controls systems, disrupt key services and cause massive machines to self-destruct. Most control systems are vulnerable to cyber attack because of their age and configuration, and because they are often connected to the internet in ways that lets' them be attacked from anywhere on the globe. When you ask many critical infrastructure companies if their control systems are connected to the internet, most will tell you that they are not. If you then examine their systems, you will find connections that they do not know about. Hackers can find these connections and use them for attacks. One DHS review found that every critical infrastructure company it examined had been penetrated and that he attackers had been lurking in the computer systems for an average of eighteen months.

Companies will not provide cybersecurity adequate for national security on a voluntary basis. A company may not know of the vulnerability, it may underestimate the threats it faces, and it may have no desire to spend money on security when this does not generate a return on investment. There is no disagreement that burdensome, prescriptive regulation should be avoided, but a reliance on voluntary or widely accepted business practices – what we do today – will damage national security. The best alternative to both prescriptive regulation and inadequate voluntary practices is a pragmatic, standards-based approach that sets goals and then lets companies decide how best to achieve them.

There are now standards and practices, building on research carried out by the National Security Agency. If they are put into practice, they can significantly reduce cyber risks. The effectiveness of these new approaches to defense can be measured using data collected from networks rather the collection of anecdotes and fables we have use in the past. We can test what works and what does not. Government can base a regulatory approach to critical infrastructure on these standards and practices. There must be decisions about which infrastructure require regulation and how regulation should be implemented, but any nation that does not put this kind of safeguards in place will ultimately be vulnerable.

The telecommunications sector is one of the truly crucial infrastructures for cybersecurity. It is the backbone of the internet and the fabric that connects us. An examination of this sector shows the complexity of the problem. The sector is already heavily regulated and it is in the business interests of major telecommunication's companies to provide reliable service. Their business models makes them the only sector with the expertise and incentives to take cybersecurity seriously, but even then there are issues and problems were uncoordinated private actin is inadequate and government intervention is needed. We may not need more regulation as much as we need insight to ensure that companies are performing at equivalent levels and to understand what threats they see.

Government needs to play a role in incentivizing and coordinating an industry wide response. An example of this kind of problem involves securing the Domain Name System – known by the term DNSSEC. DNS is the addressing system of the internet. If there was some disruption to DNS, the internet would slow to a halt or attacker would be able to hijack traffic. The problems with DNS were discovered about twenty years ago. Solutions were identified a decade ago, but the U.S. has been slow to implement them. This is beginning to change, but unevenly. Government agencies can play a coordinating and incentivizing role to promote the widespread adoption of DNSSEC, and reserve intervention only if this coordinating approach proves inadequate.

Botnets are another problem that might not require regulation. Many consumers may be unwittingly running malware and their computers may be part of a "bot." Such botnets may be used to send spam or engage in illegal activities that do not raise critical infrastructure concerns. But they may also be used to launch denial of service attacks against critical infrastructures and, in any event, create enough traffic on the network to make more egregious activity harder to detect and respond to. The ability to address infected consumer machines -- and botnets in particular -- is an important part of any critical infrastructure protection strategy.

Government agencies, the IT industry, and concerned citizen groups have engaged in a myriad of activities designed to help manage such consumer risks. They have worked to educate users about common threats and how to mitigate them, providing advice on firewalls, anti-virus, and patching. Tools have been built to automatically scan machines, patch programs, update virus signatures, and remove malware when found. As helpful as education and these tools are, they have proven to be inadequate to the task. Some consumers do not follow the guidance provided and engage in other unsafe actions. Most consumers have no desire to become IT professionals, let alone security experts, and information technology is complex enough that knowing how to protect oneself is not intuitive. As a result, many consumers may be unwittingly running malware and their computers may be part of a "bot., and computers in the U.S. are a leading source (if unwitting) of global malicious activity because of poor cybersecurity.

In this instance, the U.S. could adopt a model similar to what Australia has done to improve consumer safety. Australian ISPs have a voluntary code of conduct to protect consumers from malware and to deal with bot-nets and other consumer level problems, but this was adopted only with the strong encouragement and participation of the Government. If the companies had failed to adopt coordinated voluntary measures, there would have been regulation. The U.S. needs a similar voluntary code of conduct for ISPs, backed by government oversight, and developed using a similar voluntary and coordinated mechanism.

In thinking about cybersecurity, we still rely too much on policies created by the Clinton Administration. The 1998 Presidential Decision Directive-63 was a foundational document for cybersecurity, but the concepts and policies found in it are no longer adequate for a critical global network. PDD-63 believed that adequate cybersecurity could be achieved through voluntary measures, information sharing and public private partnerships. This may have been enough for the early days of the internet, but it is no longer sufficient.

The internet of the future will be a service. People will connect using "apps" and mobile devices whose programming will not be easily accessible to them. This will shift responsibility for security away from the "edge."
The internet will increasingly be "device-centric," further automating machines (like cars) and services without requiring constant human intervention. Commercial service providers will be at the center of the new internet, and without regulation similar to what we now use with airlines and safety of flight, public safety will be at risk.

The central problem for the U.S. will be redefining the role of government. There are clearly areas where the government should not interfere. At the same time, cybersecurity is a national security problem that requires more government involvement, not less. We often hear that the private sector owns eighty or ninety percent of the infrastructure. This idea is a leftover from the dot.com era and not very helpful. A better way to think about cybersecurity is that the private sector owns ninety percent of the targets. We do not ask airlines to protect our airspace and no one says that because the private sector owns eighty percent of beachfront property that we do not need a navy. The same logic applies to cybersecurity. You will sometimes hear that the best hackers are outside of government. Even if this is true, those hackers do not have millions of dollars in resources, access to advanced technology and other kinds of, including human spies,

and thousands of compatriots all working to undermine our defenses.

Porous technologies and weak governance make cyberspace an environment that is easily exploited by malicious actors. While we will see technological improvements over the next few decades that will reduce risk, near term improvements require changes in national policy and international cooperation. There are things we could do this year that would reduce risk, if we choose to do them. A comprehensive approach to cybersecurity can make us safer and let us take advantage of the new technologies in ways we have yet to imagine.