Testimony
Committee on Homeland Security
Subcommittee on Oversight, Investigations, and Management America is Under Cyber Attack:
Why Urgent Action is Needed Tuesday, April 24, 2012,
James A. Lewis, Center for Strategic and International Studies

Every week –it's getting kind of boring – we read about hackers pilfering some company's data base and stealing data on thousands or even millions of individuals. These are private sector networks and they point to a crucial problem for assessing cybersecurity. Government agencies have to be transparent about breaches. Companies have to report breaches when it affects consumer privacy. But companies don't have to report breaches involving intellectual property or critical infrastructure. In fact, it is in their interest to conceal them. Perhaps the new Security and Exchange Commission Ruling that asks companies to report cyber incidents that damage shareholder value will change this, but it is too early to tell.

So we have frequent reports of penetrations to governments systems, weekly or daily reports of penetrations of company networks that affect privacy, and almost no reports of penetrations affecting intellectual property and critical services. This pattern is not credible – the level of privacy-related penetrations companies report is likely to also be the real level of intellectual property-related penetration. It's just not reported. We know from anecdotal data and from a few published instances that these network penetrations occur frequently. This anomaly in the reporting suggests we really lack – in open source information - a clear understanding of the threat to the American private sector, and that protestations that private networks are secure or do a better job are, to put it charitably, inaccurate.

An accurate assessment of threats in cyberspace is essential for effective defense. A defense built on fictions will fail the first time it is tested. There is too much wishful thinking and complacency in the face of a threat that is growing as potential attackers acquire new capabilities and as our economy becomes more dependent on the internet and other cyber technologies. Digital networks are now the backbone of economic activity and natonal security, but our efforts to secure them remain haphazard, putting our natoin at risk. We can better understand this risk by looking at three seperate categories of threat – espionage, crime and attack.

Our adversaries include powerful states, skilful criminals, and a range of extremist groups. We are hampered in our defense against these opponents when we try to treat cybersecurity as a business problem. Some companies will take adequate defense measures; other will not. It makes business sense for an inteligence agency to spend lavishly to penetrate an opponent's network. It does not make business sense for comapnies to spend at the same rate to defend. To put this in military terms, we have a uncoordinated defense that is easy to defeat in detail.

Cyber espionage is the most pressing threat we face. The loss of intellectual property and business confidential information – economic espionage – using hacking and other techniques poses a threat to national security by undermining the military advantage provided by technology and by damaging economic competitiveness. The rate and degree to which national security is damaged depends, of course, on the ability of the acquiring nations to actually use the technology they steal and on America's own economic policies and government support for

science and engineering – our own economic policies and laws probably do more damage than cyber espionage - but there are many troubling incidents that suggest that real harm is being done. A major oil company lost exploration data worth hundreds of millions to a foreign attacker. We all know the Google case – at least thirty-four other high-tech companies were also penetrated, although they did not report the fact. Foreign hackers took IMF and G-20 documents relating to global financial negotiations. The delays and cost overruns in the F-35 program may be the result of cyber espionage, as could the rapid development of China's J-20 stealth fighter. Industries as diverse as chemicals, telecommunications and solar energy have all suffered from cyber espionage.

The most harmful form of cyber espionage is state-directed. Foreign nation-state opponents are sophisticated intelligence agencies and advanced militaries whose business is to defeat network defenses and who have a demonstrated capacity to easily exploit commercial and government networks. They have resources and persistence and their work can be seen as an extension of traditional espionage activities. Our network defenses are so poor, particularly in the "dot.com" space, that the effort to break in probably only takes these agencies and their proxies a few months of effort.

There is no convincing estimate of the cost of economic espionage to the United States. One study put the cost at perhaps $30 billion a year (in 2011 dollars) but other studies estimate the loss to be in the hundreds of billions. These higher figures exaggerate loss, but whatever the dollar figure, the illicit acquisition of technology and the loss of confidential political and business information hurts American security. The insight into government policies, and strategic industries provided by cyber espionage, and the acceleration of competitor technological development, provide foreign competitors with a tangible advantage that harms the United States. The Committee may wish to ask, for example, for classified briefing on improvements in China's stealth and submarine capabilities and the possible relation between these improvements and hacking incidents at defense contractors over the last decade.

We do not want to assume that losses are distributed evenly across all sectors of the economy. State sponsored espionage will focus on area of concern to governments: advanced technologies in aerospace, materials, information technology, and sensors, as well as commercially valuable financial data and energy related information. Semiconductors and solar energy have been prime targets recently. . Private entities also engage in cyber espionage, in many cases they do so with the acceptance of their governments. Hacking by private companies and individuals could engage a much broader swath of companies and technology. This probably reflects not only commercial interests but also an official policy to encourage the illicit acquisition of technology as a way to promote economic growth.

Cyber espionage ranks first as a threat to the U.S and other developed countries. Cyber crimes focused on financial gain are a lesser threat, but they damage public safety by putting private citizens and companies at risk of monetary loss. Anecdotal evidence suggests that crime against banks and other financial institutions probably costs the United States a several hundred million dollars every year. This is not a major economic loss, but harms American citizens and does some damage to our economy. However, cyber crime also threatens national security in that it allows potential opponents to maintain and train proxy forces at our expense. Nations like

Russia and China are sanctuaries for cybercrime because it allows them to maintain "irregular forces" in cyberspace – hackers who can be tapped to do the states bidding in espionage, coercion, or attack.

A recent opinion piece in a leading newspaper illustrates how confusing the discussion of cybersecurity has become, and helps explain why America may be too slow in constructing adequate defenses. The essay posited that most cyber criminals did not make much money, and that the threat they posed was overblown. You can test this formula by applying to it mugging: most muggers do not make much money, so by the same logic, mugging is not a problem. This formula is divorced from any serious concept of public safety. Similarly, the national security implications of cybercrime were overlooked. Since cyber criminals are the proxy forces – the irregulars – that our two most dangerous opponents in cyberspace use for national ends, cyber crime is an indirect and unwitting subsidies from American companies to foreign military and intelligence services.

Cyber espionage and crime happen on a daily basis. This is nto the for cyber attacks against critical infrastructure or services, whch have been few and far between. The threat comes from the spread of attack capablities. In 2007, tests at the Idaho National Labs showed that sending malicious instructions via computer networks to the industrial control systems used to run critical infrastructure could cause machines to destroy themselves. Stuxnet produced a similar effect. These incidents showed that software can be sued as a weapon, and the internet as a delivery vehicle. Espionage and crime exploit vulnerabilities in networks technologies; attacks on critical infrastructure compound this by exploiting not only network vulnerabilities but also the vulnerabilities in industrial control systems. There is no economic incentive to fix these control vulnerabilities because they will not affect normal operations and they will become visible only when there is an attack. While the cost of cyber crime is realtivley small, it is an integral part of other, more dangerous threat we face, inlcuding the ablity to launch a damaging cyber attack.

These attacks havee been long prophesied, but we have only seen two or three. Only a few nations have the capability to destroy critical infrastructure and they are unlikely to use it outside of a war. We know that our two most likely military opponents have the capability to penetrate networks, scramble data, disrupt critical services and even cause physical damage. We also know that they are more deterrable, more responsible, and in the case of China, face major disincentives, as a disruptive cyber attack would do as much damage to their own country, given how deeply our two nation's economies are intertwined.

You sometimes hear analysts say that we are in a covert cyber war with China. This is inaccurate. We should stop trying to cram our complicated relationship with China into a simple Cold War framework. China and the U.S. are interdependent in ways that were inconceivable for the U.S. and Soviet Union. China is challenging the U.S., but it is not a peer-competitor. Although it is rapidly increasing its military capabilities, it does not pose the existential threat to the United States that the Soviet Union posed. Given the deep distrust and hostility between the two nations, and the comeptitoin for regional and global influence, cybersecurity is a potential flashpoint in the bilateral relationship and a source of growing tension, but this is not war.

The number of nations seeking to acquire cyber attack capabilities is growing rapidly – cyber

attack is becoming a standard element in military planning. A more troubling development is that new classes of opponents are seeking the ability to launch cyber attacks. These new classes of opponents will not be as easily constrained. They are more likely to use cyber attack and all evidence suggests that we have nothing in the way of adequate defense. We simply do not take the threat of cyber attack seriously – would anyone not paid to do so argue that information sharing and voluntary action would protect us from terrorism? Or that telling companies what missiles and aircraft look like would be an adequate defense against a nuclear strike? But it is an American tradition to be surprised by opponents and only take action after the first attack.

The area of greatest concern is in the diffusion of the ability to attack critical infrastructure, to less responsible and less deterrable actors who may calculate that it is in their interest to launch a cyber attack against the United States. Attack capabilities could spread if private hackers to independently discover the techniques currently possessed by governments. Some members of the hacker community have amazing capabilities. Another way attack capabliteis could spread would be for hackers who are government proxies in Russia and China to "commercialize" the skills and tools they have been provided for official purposes. These proxies receive training and support from military and intelligence agencies. They also participate in the cybercrime black markets. The flow from government agencies to proxies to the black market is likely, although it appears that governments still reserve the most advanced attack technique to themselves.

It is difficult to assess how rapidly attack capablities are growing outside of governments, and the actual transmission mechanism for cyber attack tools is unclear. For example, more than a decade ago, foreign intelligence agencies had the ability to activate cell phones and use them as listening devices even if they were turned off. Variants of this technique appear to be entering the black market. We do not know if it is because someone is commercializing a skill they learned from government service or if it is an independent discovery. People play with the technology and code – this is the original meaning of hacking - and find how to do interesting things the designers never intended or suspected were possible.

The most advanced exploits are still out of reach, however, for all but large, well-resourced attackers. Stuxnet, for example, combined deep engineering knowledge and clandestine intelligence techniques with advanced hacking skills. Private hackers and most governments do not yet have the capability to launch a Stuxnet-like attack (but this is coming). That some of the Stuxnet code is publicly available does not really increase risk. Many cyber attacks are 'single-use" exploits that work as a surprise but are much less effective after the target reacts and adjusts. In the United States, for example, a 2010 survey found that three quarters of American utilities said they had put in place defenses against Stuxnet. These utilities would most likely be able to deflect a Stuxnet-like attack, while only the others would still be vulnerable.

Stuxnet has increased risk as it has shown the world how to stage a damaging cyber attack, but there are many options other than Stuxnet. Unfortunately, even private hackers can exploit freely available information on vulnerabilities and penetration techniques to attack many commercial networks and the critical infrastructure connected to them. Why use an advanced attack like Stuxnet when a simple attack will work so well? There are tools that allow anyone to scan the internet to find unprotected digital devices at critical infrastructure facilities that connect control systems to the internet. You can scan for devices that are improperly configured, devices

such as wireless routers that come from the manufacturer with the password set as 'password." It does not take a mastermind to break into such systems.

Thes tools are widely available. Informal tests using these tools can find several thousand insecure connections in the U.S. on any given day. They provide a "consumer version of the cyber reconnaissance an advanced power would carry out in planning an attack against the United States. Combine these publicly available reconnaissance tools with attack tools available on the cybercrime black market, and anyone with sufficiently advanced hacking skills will be able to attack poorly defended critical infrastructure or other commercial targets.

The diffusion and consumerization of attack capabilities is not the only growing source of threat. We must also consider motivation and intent, in addition to capability. The few nations that currently possess advanced cyber attack capabilities are deterred by American military force or they are our allies. Most cyber criminals only engage in actions that generate income. Attacking critical infrastructure does not generate income unless extortion is involved (by threatening to disrupt services if the criminal is not paid). Cybercriminals have no motive to launch a cyber attack unless they are acting as government proxies or unless they have been hired as mercenaries.

This is where the nexus between the diffusion of attack capabilities and intent become important. There are countries and groups that would like to attack the United States and are not as deterrable as our current adversaries. As nations and hackers develop more sophisticated attack capabilities and as sophisticated attack tools become available on the cybercrime black market, the threat of attack is increasing.

We know that two countries hostile to the United States are developing cyber attack capabilities. North Korea has been pursuing cyber capabilities for more than a decade but the backwardness of its economy has so far limited its success. North Korea lacks easy access to advanced technologies. Its tightly controlled population is an unlikely source of hackers, as North Koreans do not have the independence and internet access hackers need to thrive. Technological backwardness and political culture are major oobstacles to developing strong hacking capabilities, but, as with nuclear weapons, if North Korea is able to support sustained investment in cyber attack capabilities and find some outside support, it will eventually acquire them. North Korea's erratic behavior suggests it will use cyber attacks against South Korea, Japan, or U.S. forces in Korea, should it succeed in its long quest to obtain a cyber attack capability.

Iran is a more troubling case. Iran has also been pursing the acquisition of cyber attack capabilities for several years. Iran has been for many years willing to attack U.S. forces and embassies in the region, and FBI Director Mueller stated in recent testimony that Iran is more willing to carry out attacks inside the United States. Statements by Iranian officials show that they believe that the U.S., along with Israel, was responsible for the Stuxnet attacks and suggest that they believe they would be justified in retaliating in kind. Iran's attack capabilities are still limited but they have probed Israeli networks in what appear to be tests. Iranian hackers have greater access to the internet and to the cyber black market than North Korea, suggestng that their development of cyber capabliteis will be more rapid.

Iran, even more than North Korea, could miscalculate the costs of a cyber attack against the United States. Iran has groups that it sponsors, like Hezbollah, that it has used in the past to attack Americans. The Iranian may believe that these proxies will make it difficult for the U.S. to attribute an attack and this will reduce their perceptions of the risk of a cyber attack on American targets. Iran routinely exaggerates its military capabilities and its claims of cyber prowess are dubious, but there is a clear commitment (as with nuclear weapons) by the regime to continue its efforts to acquire the ability to launch cyber attacks.

Finally there are non-state, anti-American and activist groups that already make extensive use of the Internet. As cyber attack capabilities become "commoditized," the temptation for these politically motivated groups to use them against vulnerable U.S. targets will increase. We have not seen terrorist groups use cyber attacks – they seem to have neither the capability nor the interest – but since these groups make extensive use of the internet they could eventually be attracted to cyber attack if the means to carry it out are easily available. Some non-state actors are grouped under the label "Anonymous," a disparate and decentralized federation of internet activists where many members espouse anti-government or anti American ideas. The name "Anonymous" is misleading, however, as it implies a single entity. Anyone can say they are "Anonymous," from individuals posting comments on 4Chan to members of foreign intelligence agencies (for whom "false flag" operations are routine). In a few cases, it appears that cyber criminals have used the name Anonymous when carrying out their for-profit exploits.

These threats are all external, but greatest threat to America's cybersecurity come from inside. This threat is complacency and it has two sources. In the internet community, there are many who still believe that the internet can heal itself, that civil society and multistakeholder interent governance will ultimately provide adequate security. They say that threats in cyberspace are exaggerated and that better cybersecurity puts privacy and the alleged virtues of an open internet for innovation at risk. This is simply naïve amd outdated. This sort of approach has never worked anywhere else, and it is not working now in cyberspace.

At the same time, business groups underestimate the threat we face and continue to assert that some sort of disaggregated, voluntary approach to cyber security, guided by better information sharing, will be adequate to protect the nation. This, of course, was the approach adopted by the Clinton Administration in 1998. It did not work then and it does not work now. It will not work in the future when our opponents are even more advanced and when we are even more dependent on cyberspace. Simplifying the regulatory and tax structure would be immensely beneficial for our economy, but it is a non-sequitar to argue that blocking mandatory standards for cybersecurity somehow compensates for any over-regulation of commercial activities.

The future of threats in cyberspace will involve the diffusion and commoditization of attack capabilities. It will involve an increased number of privacy breaches and the loss of intellectual property and confidential business information. The situation is not static and could change rapidly. There are a number of steps we could take to reduce risk, but these steps face insurmountable political obstacles that will not disappear until after a damaging cyber event. To prepare itself for the inevitable, the Committee may wish to ask for a classified briefing on the best available intelligence estimate for when America will experience a cyber attack.