House Armed Services Committee
Subcommittee on Terrorism, Unconventional Threats and Capabilities
"Holistic Approaches to Cybersecurity to Enable Network Centric Operations"
April 1, 2008
James Andrew Lewis
Center for Strategic and International Studies

I thank the committee for the opportunity to testify. As you know, we have seen new domains for conflict emerge in the last decade. These new domains are in space and in cyberspace. Cyberspace is in some ways the more interesting of the new domains, because the 'price of entry' is low and also because it has been an area of significant U.S. vulnerability for many years, a vulnerability that has been eagerly exploited by our opponents.

We know that networks and information technology improve performance for both businesses and for militaries when they are used to provide better information and better coordination. One study examined exercises that pitted networked F-15s against F-15 relying only on traditional voice communications, and found that networking resulted in dramatic improvements in combat effectiveness.[1] This study is indicative of the direction that future conflict is likely to take – the side with the informational advantage is more likely to win. We are only at the beginning of finding the organizational structures and tactics that will make full use of the new technologies that can provide informational advantage.

But at the same time, the use of these technologies has created serious new vulnerabilities. These vulnerabilities are the result, in part, of the newness of the technologies themselves. Our opponents have seized the opportunity created by these vulnerabilities to engage in an extensive espionage campaign against the U.S. by mapping the vulnerabilities of our networks, accessing U.S. computers through these networks, and transferring sensitive information from the U.S. to their own computers.

There is also the possibility that when an unknown intruder has accessed a U.S. computer to steal information, he or she has also left something behind. We cannot say with assurance that a network that has been penetrated has also not been infected with hidden malware that could be triggered in a crisis, disrupting data and communications. This is not the "electronic Pearl Harbor" scenario that unfortunately dominated much of the early thinking about cyber security, but the potential for disruption and at least a temporary military advantage for an opponent as a result of attacking U.S. computer networks cannot be discounted.

None of our opponents will deliberately seek conventional military conflict with the U.S. Instead, they are attracted to asymmetric attacks, which look for and exploit areas where they are strong and the U.S. is weak and unaware. To achieve asymmetric advantage, some opponents will rely on terrorism or insurgent tactics, where combatants blend with the civilian population to attack the U.S. Other opponents plan to disrupt, destroy or deceive U.S. sensors and

[1] Daniel Gonzales, John Hollywood, Gina Kingston, David Signori, "Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16," RAND, 2005

communications, to degrade our informational advantage. Their goal is to exploit vulnerabilities, places where U.S. assets are poorly defended.

Computer networks are just such a place. The nature of information technology and the internet means that in these asymmetric attacks in cyberspace, the advantage lies with the attacker. The internet was not designed to be a global network with millions of different devices all interconnected over a telecommunications backbone. The result is that there are many avenues for attack. Many different entities are exploring how to take advantage of vulnerabilities in cyberspace. These include nations, criminals, terrorist groups, political activists and perhaps even some corporations.

China and Russia are perhaps the most dangerous of our potential opponents. China has resources and is willing to spend them, and Russia has experience and skill. However, China and Russia are not the only nations interested in and capable of waging cyber warfare, nor are nation-states the only potential opponents in this new domain. The emergence of a powerful and skilled cybercrime community has serious implications for U.S. interests.

Over the last few years, cyber criminals have become technologically sophisticated and well-organized. These are not the amateurs of a few years ago. Cyber criminals have developed black markets where you can buy malware, guides to vulnerabilities, credit card numbers. There are contests among cyber criminals, to see who can be the first to hack a new system or to discover a new vulnerability. Some of these sites offer guarantees while others provide a rating system for potential buyers. It is possible to rent bot-nets, huge assemblies of hijacked computers to use in an attack, or even to hire hackers. As in any black market, an unwary buyer can end up being exploited, but a knowledgeable purchaser or one with resources and experience – and this customer base includes nations, companies, and terrorist groups - can find most of what they need for cyber attacks.

If we have underestimated the risks of cyber espionage and cyber crime, the risk of cyber terrorism is overstated. Terrorists do make extensive use of the global internet for recruitment, propaganda, fundraising, training, and for command and control. The ability of terrorist groups to use commercial communications networks has provided them with robust, flat organizations that are more difficult to defeat. It has provided them with a global presence they would not have been able to achieve twenty years ago. But this is not the equivalent of attacks with bombs or firearms, which terrorists prefer. Cyber weapons are not yet sufficiently lethal for terrorist use.

To date, cyber disruption and attacks on critical infrastructure remains largely hypothetical. Cybercrime and cyber espionage are the most serious problems. Cyber-espionage is a far greater problem for national security than many recognize. Last year, the U.S. government suffered a series of breaches of its computer networks. These have been attributed to China and while attribution is always difficult when it comes to cyber attacks, we should note that senior officials in the German, French and British governmental also complained about Chinese hacking during the same time as the attacks on the U.S. occurred.

Using computer break-ins for espionage has a long history. The earliest breach I know of occurred in the 1980s, when the KGB hired West German hackers to penetrate U.S. military and

research networks. There were also incidents in the 1990s involving the Departments of Energy and Defense. These incidents show that the cybersecurity problem is twenty years old, but last year we crossed a threshold in cyberattacks, with the noisy demonstrations launched against Estonia's government networks and with the massive sustained attacks – some successful – on U.S. government networks and on the networks of allied countries.

In 2007, computer networks in the Departments of Defense, State and Commerce were penetrated and had to be taken off line for repair. It is likely that other agencies suffered breaches as well. The primary intent of these attacks was to collect information. What they revealed was a remarkable unevenness in the defense of U.S. networks. Some of our government networks, usually those providing the most sensitive services – are very secure. Other networks, including some that contain information about sensitive technologies are not as secure as we would like, whether these are at the Department of Energy or State, or even the Secretary of Defense's unclassified email system, all of which have been hacked.

This series of attacks has prompted the U.S. to begin a major new initiative to improve the security of government computer systems. The Administration has reportedly issued a new, joint policy directive – National Security Policy Directive-54 and Homeland Security Policy Directive-23, which directs agencies to carry out a comprehensive federal cybersecurity initiative. Many of the initiative's elements are highly classified – some would say over-classified – But there has been public discussion of some of its elements and the Administration has said it will make more information publicly available sometime in the next few months.

We know that the initiative allocates more money and personnel to cyber security. Federal spending on cybersecurity will increase ten to twelve percent, according to press reports. The Department of Homeland Security will expand the use of its 'Einstein' system to monitor traffic in and out of Federal government networks. Einstein will be reinforced by undisclosed NSA monitoring systems as well. Building on programs initiated in the Department of Defense, the Office of Management and Budget has mandated the use of the Federal Desktop Core Configuration, a secure standardized configuration for use on all Federal Computers. OMB has also begun a "Trusted Internet Connections" initiative (TIC), which will reduce the points of connection between Federal networks and the rest of the internet from hundreds to only fifty. The U.S. is considering whether to establish new organizations to oversee cyber security efforts, and existing organizations will be strengthened. Both DOD and the Intelligence community have increased their efforts in cyberspace. The initiative has twelve separate projects to improve cyber security, including one that will look at how to improve coordination with the private sector.

These are all very positive steps, but difficult issues remain to be solved. One such issue is improving coordination with the private sector. This will be a major test for the Initiative. The U.S. has mechanisms for coordinating public and private cyber security efforts, but in some ways these are continuation of the initial programs from the 1990s, such as the FBI's National Infrastructure Protection Center (NIPC) or the Department of Commerce's Critical Infrastructure Assurance Office (CIAO). We need to rethink and improve how the government interacts, cooperates and coordinates with the private sector to assure better cyber security.

Another issue is that there is an international element to cyber security that must be addressed. These attacks on federal networks and critical infrastructure come over global networks. A national effort can provide only part of the solution. The U.S. will need to work with its allies and perhaps even with our opponents to change this. A sustained international effort could involve better cybercrime enforcement, new international norms for cyberspace, new collaborative mechanisms and, with our allies, agreed doctrine on securing networks and responding to attacks.

One advantage of better international cooperation is that it could increase the level of deterrence, at least for cyber criminals. Currently, some nations act as sanctuaries for cybercriminals. Cybercriminals who operate overseas can, with a little skill, almost eliminate the chances of being caught and prosecuted. Only international cooperation will change this.

Other forms of deterrence are less practical. It is difficult to deter by threatening counterattack if you do not know who is attacking. It is even more difficult to deter by threatening counterattack is you cannot estimate the degree of collateral damage. Attacks come over a global network to which we are all connected, and the attackers can use unsuspecting civilian computer networks, assembled into bot-nets to launch their attacks. Last year's attacks on Estonia are a good example of these problems. They are widely attributed to Russia, and in my view Russian intelligence services are almost certainly behind the attacks, yet there is no evidence to substantiate this. The attackers, a collection of cybercriminals and amateur hackers mobilized and encouraged by unknown entities used captive computers around the world, in Europe, china and in the U.S. A counterstrike against the attacking computers would have damaged innocent networks around the world. It would be a bold President who authorized counterstrikes when he or she does not know the target or the possible extent of collateral damage to friendly networks.

The attacks on Estonia highlight the problems of anonymity and attribution. The Internet is too anonymous, and too easily deceived. Identity management must be improved if cybersecurity is to be improved. This is a thorny subject, given the implications for privacy and civil liberties, but the anonymity of the internet makes it difficult to determine who is responsible for an attack or a crime, this difficulty with attribution makes it more difficult to deter attacks. Progress on measures such as HSPD-12.which will improve Federal credentials and authentication is crucial. The RealID program, although widely vilified, is also crucial for improving the quality of identity documents and procedures in the U.S. DOD has been a leader in better identity management with its Common Access Card Program

Federal organization remains a challenge. The slow pace of the rollout of the Initiative was due in part to disagreements over which agency would have the lead. The Intelligence Community has the best capabilities for cyber defense in many ways, but there are civil liberties concerns and clear links to the renewal of the Foreign Intelligence Surveillance Act (FISA) over assigning the Director of National Intelligence the lead role. There are also concerns over giving the lead in cybersecurity to a military organization, such as the U.S. Strategic Command. The Department of Homeland Security, the civilian agency with the responsibilities for cyber security, would be the logical lead but there have been questions about its competence and authority. The previous administration had a cyber 'czar,' who successfully began the immense effort required to reorient

Federal policy and to develop strategies, but a "Czar" may no longer make sense now that the Department of Homeland Security has been created.

Government organization for cybersecurity reflects a larger challenge for the U.S. In effect, we have a vertical organization trying to respond to a horizontal threat. This means we have four or five different and independent agencies each of whom are responsible for a part of the problem. There is no single agency responsible for the entire problem. Even at the White House we have two organizations – the Homeland Security Council and the National Security Council - that share responsibility for cyber security.

This sort of organizational problem is very difficult for governments to overcome. The creation of the Department of Defense in 1948 was an effort to develop collaborative and "joint" action to meet the problems of National Security. That effort was reinforced and given new impetus by the Goldwater-Nichols Act. DOD has worked for decades to achieve 'jointness.' Other agencies are far behind in achieving a collaborative, 'horizontal approach. The creation of the Department of Homeland Security can be seen as an effort to duplicate the 1948 solution for homeland security. The Intelligence Reform and Terrorist Prevention Act can also be seen as an effort to create an 'intelligence enterprise' with a powerful CEO whose remit would stretch across multiple agencies.

I would wish reorganization on no administration, but the structure of our government is still largely based on a template created in the 1900s. This template is inefficient in many ways. Reorganization is unavoidable, but it will take years of effort. We do not have years, however, to respond to the new security threats in cyberspace.

To be fair, this problem extends beyond government. Our conceptual framework for thinking about security has moved beyond the cold war, but not by much. My concern is that conflict in cyberspace is seen the way that airplanes were seen in 1912 – interesting toys, but not a serious security or military issue. Some, pointing to Pearl Harbor and to 911, say that we will only reshape our thinking and our organization to deal with cybersecurity after some disaster has occurred. I hope this is not the case.

Federal organization, strategy and doctrine, coordination with the private sector and allies – these and other issues remain challenges despite the progress made by the President's cybersecurity initiative. That the initiative comes in the last year of the Presidency also creates challenges. Any administration would face difficulties in making rapid progress on a new initiative after July. The political realities are that the Administration has between fourteen and sixteen weeks to implement its cyber initiative. Much can be done, but much will necessarily remain unfinished.

This means that the burden of improving cybersecurity will fall on the next administration when it takes office in January of 2009. That administration, whether Democratic or Republican, will inherit a cyber security situation that is much improved. It will also inherit a cyber security initiative that is a work in progress, with a number of unfinished elements. Like any new administration, it will have to ask what should it keep or continue from this initiative, what should it change or drop, and what new steps it should take to address this increasingly serious problem for national security.

Transitions are also, as the members of the Committee well know, a moment of opportunity. The new Administration will have a degree of good will and authority. Perhaps more importantly, it will have something of a clean slate when it comes to initiatives and organization. 2009, the first year of the next administration, provides an opportunity to take the Bush Administration's cybersecurity initiative and advance it.

To help the new administration think about this opportunity, The Center for Strategic and International Studies (CSIS) established a nonpartisan commission on Cyber Security for the 44th Presidency – the administration that will take office in January 2009. CSIS is a nonpartisan, nonprofit research organization headquartered in Washington, D.C. with more than 200 staff and a large network of affiliated experts. Its focus is on security in a changing global environment. CSIS's has been conducting research, holding public events, and advising government agencies on cyber security since before 2000, and this body of work will provide the foundation for the Commission on Cyber Security for the 44th Presidency. CSIS routinely uses commissions, task forces and work groups to help it conduct analysis and develop recommendations. This approach lets us draw upon the broader communities of interest in Washington and benefit from their expertise and experience.

The goal of this effort is to look at cybersecurity as a problem for national security and develop recommendations for a comprehensive strategy to improve cyber security in federal systems and in critical infrastructure. The Commission will consider federal organization and strategy, cybersecurity norms and authorities, international issues, federal investment and acquisition policies, and it will explore ways in which the government can engage with the private sector.

The members of the commission are experts in cybersecurity with extensive government experience. In addition, CSIS intends to make the work of the Commission an inclusive process and has asked other experts and groups to participate in the development of recommendations and to make plenary presentations on substantive issues. Our first public briefing took place on March 12, in a well attended event where five widely recognized leaders in cybersecurity give their views and recommendations on how to move forward in cybersecurity. We plan to hold several more briefings in the next three months.

As part of this effort, we have created a number of working groups that will examine these issues in detail and develop specific recommendations. These groups have just begun their work. They include members of the commission and other experts, all of whom have volunteered their time for this effort. If the committee wishes, I can report back at a later stage on how their work has progressed. Our plan is for the Commission to complete its work by November 2008. The final product from the Commission will be a well-supported package of recommendations for improving cyber security that could help to guide U.S. policy in the future.

The advantage we gain from being network centric is eroded by uneven security. We will never have perfect security, but our goal, as a nation, should be to increase our ability to use network technologies to improve our military and economic performance while at the same time reduce the ability of our opponents to take advantage. Our hope is that the efforts of CSIS and the other participants in the commission can contribute in some way to this improvement.

One element of the CSIS projects is to reassess the larger strategic context for cybersecurity. This context is shaped by considerations involving national defense, law enforcement, intelligence and global economic competition. This may require a broader definition of national security. It is no surprise that one result of immense economic and technological change we are undergoing is that old assumptions about security and the policies based on those assumption do not work as well as they did in the past. The process of adjusting those policies to the new global environment is a major challenge for all governments. Each country in some way must respond to a world where the lines between government and commercial, and between domestic and foreign are blurred. This blurring makes finding solutions to cybersecurity more difficult but achieving better cyber security and greater benefit from network centric operations requires this reassessment of the strategic context.

In the 1990s, there was considerable discussion of what the international security environment would look like after the cold war and what the new threats to US security would be in that environment. Much of this speculation was wrong, not in that it misidentified the new threats, but that it gave some threats more importance than they deserved. We underestimated the threat of global terrorism. We did not prepare adequately for cyber espionage. There were a few visionaries who pointed to these problems, but in the main, they were ignored.

In the last decade, the shape and nature of the new security environment has become clearer. We face new kinds of competition and new kinds of threats. In this new environment, the ability to operate in cyberspace and to defend against the operations of others in cyberspace is a crucial task for security. The United States has begun to take the steps needed to defend and to compete effectively in cyberspace, but we have only begun and there is much to do.

I thank the Committee again and I would be happy to take any questions.