HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE

September 19, 2008

BY PAUL B. KURTZ

PARTNER, GOOD HARBOR CONSULTING

MEMBER OF THE CSIS COMMISSION ON CYBERSECURITY

Thank you Chairman Reyes and Ranking Member Hoekstra for inviting me to testify before you today.

Cyber security is one of the most serious economic and national security challenges we will face in the 21st century. U.S. Government leadership is vital to mitigating massive problems with our information infrastructure.

Our current information infrastructure is riddled with holes, unknown backdoors, and is extremely difficult to protect in the face of increasingly sophisticated adversaries. Unlike Y2K, there is no single fix. Adversaries are not limited to nation states' military and intelligence organizations. Criminals, organized crime, terrorists, malicious insiders, and business competitors can and do engage. The battle in cyberspace is just beginning. It is destined to be complicated and costly.

There is an urgent need to understand the problem and set the foundations for a more secure, reliable, resilient information infrastructure that can operate in an increasingly hostile environment.

The absence of concerted leadership by the U.S. government will yield continued loss of intellectual property, slow our economy, and impair both our competitiveness and national security.

American industry and government are spending billions to develop new products and technology that are being stolen at little to no cost by our adversaries. Nothing is off limits—pharmaceuticals, biotech, IT, engine design, and weapons designs. It is not just intellectual property (IP) at stake—information ranging from personal financial data, troop deployments and emergency response programs, to company staffing is at risk.

The long-term threat involves the disruption of critical services through attacks against financial, utilities, transportation, and logistics systems. Control systems supporting utilities—power generation and transmission, oil, gas, and water distribution are vulnerable. The integrity of data is also at risk. Adversaries can penetrate systems altering or manipulating critical data. The consequences of such attacks would be disastrous, for example, misinforming key decision makers at a time of crisis.

The role of Intelligence Community (IC) will be vital as we move forward. It must not only understand plans, program and intentions, but it also it must also be ready to be called upon to help determine attribution when attacks occur.

Today I have been asked to cover three areas associated with this national security challenge: the Center for Strategic and International Studies (CSIS) Commission on Cyber Security for the 44th

Presidency; the President Bush's Comprehensive National Cyber Initiative (CNCI), and cyber espionage.

CSIS Commission

Over a year ago CSIS established a non-partisan commission co-chaired by Representatives Langevin (RI) and McCaul (TX) to offer recommendations to next president on how to improve cyber security. Under the excellent leadership of Jim Lewis from CSIS, Scott Charney of Microsoft, and Lieutenant General Harry Raduege (USAF, Ret), 35 experts on the Commission are focusing on a set of recommendations addressing the following areas:

- Leadership – Who's in charge
- Organization – What's the best organization to address the problem
- Strategy – What should be government's top priorities and how should it go about achieving them
- Regulation – What is the role of regulation in securing cyber space
- Public-private sector coordination -- How should both collaborate and share information
- Identity and attribution – How can each contribute to the improvement of security
- Authorities – What new government authorities are needed

- Research and development – What are the biggest technical challenges requiring attention
- Use of all instruments of power— How to most effectively use diplomatic, military, economic, law enforcement, and intelligence--to secure cyberspace.

The Commission will release its findings in late October. In each of these areas the U.S. Government faces significant challenges. Some recommendations are straight forward, others less so. For example, it is clear that we need a strategy and that cyber security is national security issue, not a homeland security issue. In addition, given the complexities associated with the information infrastructure, leadership is required at the most senior levels at the White House. However, determining the best place to house and coordinate *operational* collaboration across Federal agencies and with private sector requires careful consideration. The role of regulation is also being considered. For example, the Commission is considering whether Internet Service Providers and carriers should be required to scan for malicious code. Today such action is voluntary.

The unclassified nature of the Commission's product precludes a detailed discussion on military and intelligence issues associated with cyberspace. However, the Commission is in agreement that there is a very close relationship between steps to secure information systems and measures to collect and attack information systems.

Comprehensive National Cybersecurity Initiative (CNCI)

Unlike the Commission's work, the White House's classified Comprehensive National Cybersecurity Initiative (CNCI) is focused almost exclusively in the security of Federal information systems. Little public information was available about the initiative until the White House held a briefing this week given the prospect of Congressional hearings on the Commission's work. CNCI is described as a multiagency undertaking to improve collaboration across the Federal government on cyber security. The CNCI will address cyber security challenges by:

- Employing transformational technology
- Increasing situational awareness by connecting the cybersecurity centers of excellence
- Maximizing the ability to attribute cyber attacks and intrusions through exploratory research and development
- Increasing core foreign intelligence collection to provide indications and warning
- Developing the framework to create a future environment that no longer favors cyber intruders into our networks and systems.

More specifically, CNCI seeks to:

Establish a front line of defense through such initiatives as:

- Trusted Internet Connect

- Deploying passive sensors across federal systems
- Deploying intrusion prevention systems
- Better coordination of R&D efforts

Demonstrate resolve to protect us cyberspace and set conditions for long-term success by:

- Connecting key government operations centers
- Developing a government wide cyber counter intelligence plan
- Increasing the security of classified networks
- Expanding education

Shape the future environment through:

- Defining and developing leap ahead technologies, strategies and programs
- Defining deterrence strategies and programs
- Developing supply chain risk management systems
- Defining the federal role for expanding cyber security into other critical infrastructures.

Comparison between CNCI and the Commission's Work

Despite its name, the CNCI is not "comprehensive." For example, unlike the Commission's work, it does not set out a strategy or address the challenges the private sector is facing. However, it is a

worthy--if belated--start on establishing and coordinating stronger cyber security programs across the Federal government. Many agencies, including the Department of Defense, Federal Bureau of Investigation, and the Office of the Director of National Intelligence (ODNI), the National Counter Intelligence Executive (NCIX) and elements of Department of Homeland Security (DHS) provided unclassified briefings to the Commission on the Initiative despite White House staff wishes. Members of the Commission appreciate the transparency shown by these agencies and as a result many of the Commission's recommendations will build on the work of the CNCI.

The CNCI Joint Taskforce under the leadership of Melissa Hathaway has made steady progress on the Initiative over the past year despite its politicization by White House staff and bureaucratic infighting at the DHS. Even with the CNCI's shortcomings, Congress should fund the Initiative. Without adequate funding, the Federal government will continue to fall behind in our efforts to set the foundations to build a more secure, reliable, resilient information infrastructure.

Cyber Espionage

Jim Gosler—Sandia National Laboratory's leading cyber warrior—wrote in the his 2005 article "digital dimension" on cyber espionage that an insider with authorized access could exfiltrate more than a million pages of sensitive material within a microelectronic memory device the size of a hearing aid. He continued such technology was available to only a few intelligence organizations ten years ago. Now

such technology is readily available. Furthermore, the adversary no longer has to have physical proximity to the target. As an added bonus the adversary's communications infrastructure—the Internet—is free reducing the costs and risks associated with operations. The contest between offense and defense as Gosler notes is "dreadfully mismatched."

Today our information systems are being exploited on an unprecedented scale by state and non-state actors. We face a dangerous combination of known and unknown vulnerabilities, strong adversary capabilities, and weak situational awareness. Adversaries are trying to maintain a persistent, pervasive presence across our networks.

Government networks are being targeted to steal sensitive information and gain understanding of mission-critical dependencies and vulnerabilities. Corporate intellectual property across all sectors is being stolen (information technology, bio-technology, defense industrial base, financial, transportation, and energy). The NCIX has estimated that the loss of intellectual property totals in excess of 200 billion per year.

The United States is not alone in coming to this conclusion. Last year Der Spiegel published a story noting attacks against several German agencies at the hands of the Chinese. Foreign, economics and research ministries were targeted. Subsequently, Chancellor Merkel noted the danger of cyber risks emanating from China. Last December a letter was sent from the UK's MI-5 to England's top 300

companies underscoring cyber risks. The MI-5 named China and Russia as threats.

The Role of the Intelligence Community

The role of the Intelligence Community (IC) is vital in securing cyberspace as well as supporting warfighters. The IC carries its traditional responsibilities of providing indications and warning of the plans, intentions, and capabilities of adversaries.

However, the challenges for the Intelligence Community in cyber are daunting. The cyber *security* challenge for the IC has at least three distinguishing characteristics:

Technical Nature of Information

Unlike traditional collection and analysis that focuses primarily on the *substance* of communications or *visually* observing behavior, in cyberspace, the IC must collect, dissect and analyze code. Adversaries are growing more sophisticated in hiding the malicious nature of code and its functionality. This process is labor intensive, requiring new resources, capabilities, and skill sets.

Determining Attribution

Should the functionality of code be uncovered, this leaves the critical question of origin. Who developed the code and where did it come from? Was it installed remotely, or did insiders facilitate access? Internet communications routinely transit several “hops,” making it easy to hide or spoof the origin of an attack. This is an exceptionally difficult challenge to overcome. However, it is vital, as we must be

able to determine the origin of attacks, particularly if the United States intends to use military force to respond.

Scope

Finally, there is the issue of scope. The IC must think beyond the traditional target set of information systems that support government operations. In cyberspace, war is different. While government and the military systems may be targeted through cyberspace, equally if not more plausible are attacks against *privately owned and operated* critical information infrastructure supporting finance, transportation, energy, and health networks. For example, we saw in Estonia that financial networks were subject to attack and there is evidence of al Qaeda and China mapping private sector operations in the United States. This poses a distinct challenge to IC: how to establish intelligence and collection requirements to ensure we understand plans, programs, and intentions of adversaries that seek to target private sector owned and operated systems for purposes of economic espionage or war planning.

Equally important, the IC must develop strategy and procedures for sharing information with the private sector about such plans and attacks. In the counterterrorism world, there is an obligation for government to inform citizens of threat information. No such obligation exists for cyber security. Today the U.S. government is withholding information derived through intelligence channels about cyber attacks against the private sector.

While the NCIX is charged with the responsibility of leading counter-intelligence efforts for both the government *and* the private sector, it appears that the authority, resources and capabilities to address the latter are wholly inadequate. For example, if the IC learns that U.S.-based auto manufacturing company is a target of state or industrial-sponsored espionage, the NCIX has real limitations in providing information to the targeted firm and industry that would help it defend against the attacks. Offering information on what ports to block is simply not enough. Adversaries are seeking to establish a persistent presence and using increasingly sophisticated command and control means to piggyback on legitimate applications.

This Committee could be of great assistance by asking for a full briefing from the NCIX, FBI, CIA, NSA and other relevant agencies in the U.S. Government on how to address the growing problem of adversary exploitation of privately owned and operated computer networks. Clarity is needed on the authorities and procedures governing information sharing with the private sector. This committee should convene roundtables with the private sector to discuss the attacks they are experiencing at the hands of unknown adversaries and to learn more about what if any information they receive from the Federal government about such attacks.

Procedures are needed to ensure the provision of information does not favor one company over another and “sources and methods” issues that must also be addressed. However, it should not be acceptable for the U.S. Government to not share enough information

with companies and organizations to allow them to take appropriate measures to defend themselves.

In this context, this Committee should request an annual assessment from NCIX on cyber attacks that the IC has witnessed against the private sector and the steps it has taken to inform the affected parties with sufficient information to take protective action. This assessment should be produced in partnership with the National Intelligence Council (NIC) that is responsible for producing National Intelligence Estimates (NIEs).

Finally, Congress must rationalize the current committee structure to address the cyber threat. Currently several committees in each chamber have jurisdiction. At minimum there should be a Joint Cybersecurity Committee, similar in function to the Joint Economic Committee.

In conclusion, the challenges to securing our information infrastructure are significant. The CNCI represents a beginning, but we have woefully behind and are vulnerable. U.S. Government leadership, vision, and commitment are critical.

Thank you for the opportunity to testify.