Testimony of

Larry M. Wortzel, Ph.D.

November 17, 2009

Preventing Terrorist Attacks, Countering Cyber Intrusions, and Protecting Privacy in Cyberspace

Testimony before the Subcommittee on Terrorism and Homeland Security

United States Senate

By

Larry M. Wortzel
Vice Chairman
U.S.-China Economic and Security Review Commission

November 17, 2009

Dirksen Senate Office Building

Chairman Cardin, Ranking Member Kyl, thank you for giving me the opportunity to testify today on cyber threats, security, preventing terrorist acts, and protecting the privacy of Americans.

Our nation's critical infrastructure, economy, defense information, and citizens are threatened by hackers, terrorists, and hostile foreign intelligence services. Preventing computer network penetration and pursuing those who attack us while at the same time preserving civil liberties and privacy is a challenge. Our intelligence and law enforcement agencies have been successful in preventing terrorist attacks and detecting espionage because of laws such as the Foreign Intelligence and Surveillance Act and the PATRIOT Act. With more of such legislation, and with careful oversight and attention from Congress and the White House, our intelligence agencies and law enforcement authorities can accomplish much in protecting America's computer networks.

In my remarks, I'll make reference to a report the U.S.-China Economic and Security Review Commission recently released on China's capability to conduct cyber warfare and to penetrate and exploit computer networks. The report's findings are relevant to the challenge of securing critical infrastructure and to preventing cyber attacks. And the lessons learned by preventing

intrusions from China can be applied to all other forms of intrusions, including those attempted by terrorist groups.

In addition to discussing the Commission's findings about cyber security and our recommendations to Congress, I will provide my personal views, informed by my experience as a U.S. Army intelligence officer and by my research while employed at The Heritage Foundation.

We can do better in some areas. I do not believe that the Computer Fraud and Abuse Act, even as amended by the PATRIOT Act, is yet sufficient to address certain critical issues. This includes the right of private response to computer penetrations, such as cyber counterattacks, by our government or private individuals or companies in retaliation for cyber intrusions.

As our Commission's report documents, there have been significant penetrations of our critical infrastructure, our defense contractors, and government cyber networks, including those of the Department of Defense. The Commission recommended that Congress respond by evaluating the effectiveness and the resources available for law enforcement and the Intelligence Community. Among the most important objectives should be developing reliable attribution techniques to determine the origin of computer exploitations and attacks. The Commission also recommended that Congress urge the Obama administration to develop measures to deter malicious Chinese cyber activity.

In a recent editorial, I pointed out that government and private industry are still in a reactive posture to cyber intrusions and cyber espionage. As yet, there is no fully coordinated government and industry response. President Obama made a good start with the 60-day cyber review earlier this year, but there still is no cyber security coordinator at the White House, as recommended by the White House review. Efforts to coordinate standards and policies across government and in the private sector appear stalled without the support of senior leadership in the National Security Council.

That said, I think President Obama was wise to incorporate the Homeland Security Council Staff into the National Security Council. The National Security Act of 1947 is a fine model. With proper staffing in the White House and attention from the National Security Advisor, a unified, well-led effort can bring together the agencies of the government and coordinate cyber security with allies and private industry. Also, creating the U.S. Cyber Command is an outstanding initiative within the Department of Defense.

There is still debate about what agency should lead cyber efforts and set standards. The Department of Homeland Security can help to coordinate these with state and local governments as well as private industry.

I believe the lead agency, however, should be the National Security Agency (NSA). NSA has a strong institutional culture of adherence to the Foreign Intelligence and Surveillance Act. Its personnel, like all the members of the intelligence community, are trained to protect the privacy and rights of American persons. No agency has the decades of experience the National Security Agency has in conducting operations in the electronic and cyber realms; its personnel are skilled and superbly trained; it has broad international contacts with allies and friendly governments; it

has wide contacts in the private sector; and it has a cadre of highly skilled linguists able to work in the languages associated with the origin of the foreign intrusions.

{End of Oral Testimony, written submission continues below}

Most of my recent work has been on China. Therefore as I frame the severity of the cyber threats we face, I am going highlight China as a substantial part of the problem. I recognize, however, that the concerns of this Committee extend far beyond only the malicious activities of one country. But the threat to our computer networks posed by the Chinese military, government, and individual hackers parallels the danger America faces from other countries and from terrorist organizations.

Reliable statistics about the quantity of cyber attacks against U.S. information systems are difficult to compile. But by most measures, attacks are on the rise. Take recent data from the Department of Defense (DoD) as an example: from 2007 to 2008, attacks against DoD information systems went from 43,880 to 54,640, an increase of almost 20 percent. If trends from the first half of 2009 continue through the rest of the year, attacks will have reached approximately 87,570, a sixty percent increase from 2008. This rise coincides with a large increase in attacks on other U.S. government agencies over the same period.

Each of these penetrations involves a series of actions that do not differ substantially whether the intruder is acting on behalf of a terrorist group, a foreign government, a corporation, or is acting as an individual. The severe intrusions into cyber systems involve penetrating system security, navigating and mapping the cyber system, targeting the nodes that control the system and contain the most critical data, and often, extracting the data. At the same time, an intruder might leave behind a malicious software that could be activated later to regain entry or disrupt the affected system.

General James E. Cartwright, then the commander of the U.S. Strategic Command (USSTRATCOM), told our commission in March 2007, that "China is actively engaged in cyber reconnaissance by probing computer networks of U.S. government agencies as well as private companies." General Cartwright pointed out to commissioners that the data from these reconnaissance efforts helps identify weak points in networks and that large amounts of data are extracted from systems in minutes, accomplishing in a short time what traditional human intelligence might gather over a much longer period of time. Finally, General Cartwright pointed out that the psychological effects, chaos and disruption caused by a major cyber attack could be at the magnitude of similar effects caused by a weapon of mass destruction. This last point is true regardless of what country, group, or person perpetrates an attack of that magnitude.

As alarming as these figures are, anecdotal evidence conveys the actual impact of such attacks on American targets. Time Magazine reported in 2005 about the network penetration of Sandia National Nuclear Weapons Laboratory, which may have led to the loss of information on nuclear weapons systems and other advanced technologies with weapons applications. Based on the volume of reporting, attacks like this seem to be more prevalent. The Wall Street Journal reported in April of this year about the compromise of defense contractor computer systems that contained sensitive data about an advanced U.S. fighter plane, the F-35 "Lightning II." The same

month, the paper published an article about the pervasive compromise of U.S. critical infrastructure nodes. Of course, I do not have to tell this Subcommittee about attacks over the past several years on the computers of Members of Congress such as Representatives Frank Wolf and Mark Kirk, or Senator Bill Nelson. All of the aforementioned examples have been attributed, with various degrees of certainty, to China.

China has not confined its efforts to just cyber espionage. As I stated in a recent Op-Ed in the Wall Street Journal, China's military has long sought powerful offensive cyber warfare capabilities.

The PLA has been developing these [offensive cyber] capabilities since at least 2003, when the then-director of the PLA's electronic warfare department, Dai Qingmin, proposed a comprehensive information warfare effort, including cyber attack, electronic attack and coordinated kinetic attacks in military operations.

China's military planners envision the coordinated use of this strategy--what they call "Integrated Network Electronic Warfare" (INEW)--against an adversary to gain an advantage in the early stages of a military conflict. This sort of multi-spectrum assault has potential implications that go well beyond the battlefield. Given the complex architecture of modern military command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems, there is little chance that cyber warfare would remain localized to a particular theater of conflict. Cyber attacks specifically targeting domestic civilian infrastructure cannot be ruled out, and indeed some Chinese military theorists advocate such an approach in warfare. China, therefore, bears close examination as we consider our own policies for defense.

Other countries and groups likely contemplate similar types of operations. After all, many of these concepts were based on what the United States and coalition partners did in military operations in Kosovo and both offensives in Iraq. Think about the havoc that would result if a terrorist attack of the magnitude of the one on New York and the Pentagon on September 11, 2001 were coordinated with a concerted cyber attack on U.S. civil infrastructure or our banking system. According to The Wall Street Journal we have already experienced intrusions into our electric grids that illustrate how vulnerable the nation remains, and malicious code may have been left behind.

Executive Branch Roles and Missions

The United States must actively address the challenges to our cyber security. To help stem the penetrations of U.S. companies, the Federal Bureau of Investigation has developed a defensive security education program to help private industry respond to the threat. So has the Department of Homeland Security. Executive Order 12829 established the National Industrial Security Program (NISP) to protect some 12,000 contractors that handle classified government information in the performance of their contracts. The Defense Security Service administers this program, for the Department of Defense and 23 other federal agencies. The Defense Security Service points out that "US. Industry develops and produces much of our nation's defense technology-much of which is classified."

The public-private partnership US-CERT (United States Computer Security Emergency Readiness Team) is charged with "providing response support and defense against cyber attacks for the Federal Civil Executive Branch (that is, all .gov domains) and information sharing and collaboration with state and local government, industry and international partners." US-CERT is the operational arm of the National Cyber Security Division at the Department of Homeland Security. On October 30, 2009, Secretary Napolitano opened a National Cyber Security and Communications Integration Center, designed to "facilitate a coordinated system to detect threats and communicate protective measures to ...federal, state, local and private sector partners and the public."

Still, we have to remediate some structural problems in the government's approach to securing our networks. In particular, I would like to address what appears to be an ongoing debate about the respective roles of the soon to be operational United States Cyber Command (USCYBERCOM) and the Department of Homeland Security (DHS).

As a full disclosure, early in my career, I worked on National Security Agency (NSA) programs and continued to be associated with some of them throughout my military career. Therefore, I have to admit to some bias in favor of that agency. The NSA will likely be given the responsibility of also being the headquarters of the USCYBERCOM. My personal experience with NSA leads me to tell you that I have no reservations about that agency taking the lead in implementing U.S. cyber defenses. The NSA and its predecessor organizations have continuously--and successfully--handled technical operations for our government since World War I. The Agency has decades of institutional experience, and highly skilled personnel who can operate in the electronic and cyber realms. NSA personnel also have the crucial linguistic capabilities to support investigations of foreign intrusions. The NSA has international relationships with American friends and allies and a wide range of relationships across industry. It is therefore best qualified to head the government's efforts in the cyber realm. I also want to point out that as a counterintelligence special agent, a foreign intelligence collector and a signals intelligence collector I underwent days of training and continual re-instruction on the nuances of gathering critical intelligence while still protecting the privacy rights of American citizens. Our entire Intelligence Community gets such training.

While few dispute that the NSA should direct the United States' offensive cyber operations, some cite privacy concerns over NSA involvement in securing government networks. My experience is that the NSA is extremely sensitive to intelligence oversight issues; their operators get a great deal of training and have privacy concerns drilled into their heads by leaders, inspectors general, oversight personnel, and training officers. I am very comfortable with the job that NSA does to ensure that its employees adhere to laws limiting the collection of information on United States persons.

DHS should play a substantive role in the defense of our nation's cyber space and critical information systems. To be candid, however, that Department is new, has a broad range of responsibilities, is spread thin, and is still growing into its duties. My understanding is that DHS has run two national cyber exercises. But to my knowledge, there has not yet been a systematic examination of lessons learned from the exercises nor uniform application of standards for attempting to correct any problems revealed across government or in industry.

DHS' agencies and personnel have difficult tasks before them and they are working hard to meet the challenges; but I would like to give them a little more time before saddling the Department with all of the government's cyber security responsibilities. DHS also has other challenges it has to meet to defend against terrorists and to secure the homeland. The Department is not yet inspecting a substantial portion of shipping containers or unaccompanied baggage. The US-Visit program may allow the Department to know who is entering the country and with what type of visa, but we still have no idea when or if the same people leave. I would prefer to have an agency with years of experience and success in electronic and cyber operations like the NSA take the lead.

If privacy for American citizens is a concern, also think about institutional culture. Since the time of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the 1975 Church Committee), agencies of the U.S. Intelligence Community have come under strict oversight and revised their training and operations. All of the agencies of the Intelligence Community must by law seek investigative warrants under the Foreign Intelligence and Surveillance Act to intrude into the privacy of Americans. If I remember correctly my own training as a human intelligence collector and counterintelligence special agent, some of the agencies that formed DHS could (and still can) conduct intrusive, warrantless searches at our borders or customs searches with little probable cause other than the judgment of the agent. Our laws permit such searches for good reason under certain circumstances, but I would argue that the institutional culture in some agencies of DHS is very different than that in other law enforcement and intelligence agencies.

The Public-Private Relationship

Aside from structural decisions we make in government and the responsibilities in the National Security Council and White House, we need to bring in players from outside the government. The nation's critical infrastructure is owned and/or operated by the private sector. In an October 2009 article, former acting Cyber Security Coordinator Melissa Hathaway highlighted the important role that the private sector must play to ensure our nation's resiliency in face of continuous malicious cyber activity. "Our government," she said, "must take bold steps to operationalize a partnership with industry. We need greater information sharing between the government and private sector on what is being targeted, and how."

Hathaway continued:

Our government cannot develop a strategy independent of private sector insight and cooperation. Our nation will need the private sector and its services and capabilities to find...[prevalent attack methodologies], inform the government of them and develop the solutions to resolve them. Our government needs to cultivate a public-private partnership and action plan that identifies the requirements for the future architecture, hardware, software and services that enable security and resilience. I believe that the private sector is ready to work with government on these efforts, and in order to take advantage of this opportunity, the government must actively engage the private sector and set aggressive milestones toward achieving common goals.

I would add that the government has a key responsibility here: to facilitate information sharing. This is where DHS could--and should--enable communication between all levels of government

and relevant private entities. Moreover, it is critical that comprehensive guidelines for security best practices be developed and made available to the owners and operators of critical infrastructure. Congress has levers--such as tax incentives--that it should use to promote the adoption of these practices. In the absence of significant progress, Congress and the Administration should be willing to take a more active role in overseeing better security procedures.

International Cooperation and Cyber Defense Strategy

Parallel to our efforts at home, the United States must reach out to other nations to work against cyber threats. Japan, the United Kingdom, Estonia, Germany, and Australia, for example, have all reported malicious cyber activities targeting government systems. A more formal mechanism to exchange data about attacks would be tremendously helpful for investigators and to develop defenses. Such a mechanism should be established as soon as possible. Ideally, it would be in place and tested before a major computer crisis that requires rapid information sharing. The same urgency applies--perhaps to an even greater extent--to domestic information sharing processes across government and industry. This speaks to a more fundamental change we must make in our approach to cyber security: we must be more proactive. We can and should do more to get ahead of this problem, but it will take participation from all of the relevant stakeholders, facilitated by strong and centralized coordination.

Legislative Considerations

The National Research Council recently explored a number of issues related to cyber attacks and domestic law enforcement, not the least of which is the body of legislation on cyber matters. I asked our staff at the U.S.-China Economic and Security Review Commission to put together a short, although perhaps not exhaustive, compendium for me on laws relating to cyber crimes and cyber security. I have attached their work as an appendix to this testimony.

It seems to me that one useful contribution from a legislative standpoint would be for Congress to update and coordinate these laws to ensure that all of the activities in the electronic, telecommunications and cyber domains permitted by law, as well as privacy and security considerations, are fully integrated. Also, I am not certain that implementing regulations and Executive Orders are in place to ensure effective compliance with all the legislation. This is an area where the Congressional Research Service may be able to conduct a deeper study on the efficacy of integrating the legislation or the effectiveness of Executive Branch implementation. Alternatively, an audit by the Government Accountability Office may point the way for improvements in legislation, regulation, or oversight.

Chairman Cardin, Ranking Member Kyl, members of the Committee, thank you for your time and the opportunity to think more deeply about terrorism, protecting the privacy of Americans, and cyber security.

Larry M. Wortzel is vice chairman of the U.S.-China Economic and Security Review Commission. He is a retired Army colonel who served two tours of duty as a military attaché in China. Dr. Wortzel earned a Ph.D. in political science from the University of Hawaii - Manoa. He is a graduate of the U.S. Army War College and later served as director of the Strategic Studies Institute of that institution. For 25 years of his 32-year military career, Dr. Wortzel was an intelligence officer. He had assignments in human-source intelligence collection, signals intelligence collection, and foreign counterintelligence. After retiring from the Army, he was Asian studies director and vice president for foreign policy and defense studies at The Heritage Foundation.

Appendix: Some of the Legislation Covering Cyber Crime, Cyber Security and Privacy in Electronic Communication

Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act (18 U.S.C. § 1030) was passed by Congress in 1984 and subsequently amended in 1986, 1994, 1996, in 2001 by the USA PATRIOT Act, in 2002 by the Cyber Security Enhancement Act, and in 2008 by the Identity Theft Enforcement and Restitution Act. The purpose of the CFAA is to reduce cracking of "protected computers" defined as "a computer used by the federal government or a financial institution, or one which is used in interstate or foreign commerce.

CFAA outlines seven types of criminal activity. They are listed below and have been revised according to the amendments made in 1986, 1994, 1996, 2001, and 2008:

1) Obtaining national security information from a computer without authorization and willfully communicating or transmitting the information

2) Compromising the confidentiality of a protected computer

3) Trespassing in a government computer
o This includes those individuals who have no authorization to access a "nonpublic" computer. "Nonpublic" includes most government computers, but not Internet servers that, by design, offer services to members of the general public. For example, a government agency's database server is probably nonpublic, while the same agency's web servers and domain name servers are "public."
4) Accessing a computer to defraud and obtain value
o This value must be greater than $5000 in a one year period.
5) Damaging a computer or information
o This includes both causing damage intentionally and/or recklessly.
o Damage is defined as "any impairment to the integrity or availability of data, a program, a system, or information." It includes economic loss (which can include time spent investigating and responding to attacks), threats to medical care, physical injury, threats to public health or security, and special harm to justice, national defense, or national security.
6) Trafficking in passwords
o This transferring of passwords must affect interstate or foreign commerce, or computers used by and for the United States.
7) Extortion involving threats to damage computers, steal data on the computer, publicly display data, or not pay for damage already caused
o This section applies, for example, to situations in which intruders threaten to penetrate a system and encrypt or delete a database. Other scenarios might involve the threat of distributed denial of service attacks that would shut down the victim's computers.

Wiretap Act and Electronic Communications Privacy Act

The Wiretap Act (18 U.S.C. § 2511) has as its dual purposes: "(1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized." Although the original act covered only wire and oral communications, Congress amended it in 1986 to include electronic communications under the Electronic Communications Privacy Act. The 1986 amendment made the Wiretap Act another option for prosecuting computer intrusions that include real-time capture of information.

? The core prohibition of the Wiretap Act prohibits any person from intentionally intercepting, or attempting to intercept, any wire, oral, or electronic communication. Additionally, the Wiretap Act prohibits the "disclosure" or "use" of an intercepted message.

? Congress introduced amendments to this act in 1986 which stipulate that, in order to constitute a criminal violation, the interception of a covered communication must be "intentional"--deliberate and purposeful.

? The Wiretap Act defines an "intercept" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device."

? The Electronic Communications Privacy Act of 1986 (ECPA) was enacted by the United States Congress to extend government restrictions on wire taps from telephone calls to include

transmissions of electronic data by computer. The ECPA also added new provisions prohibiting access to stored electronic communications and included so-called pen/trap provisions that permit the tracing of telephone communications.

Other Statutes
? Unlawful Access to Stored Communications (18 U.S.C. § 2701) - focuses on protecting email and voicemail from unauthorized access.
? Identity Theft (18 U.S.C. § 1028(a)(7)) and Aggravated Identity Theft (18 U.S.C. § 1028A) - applies to when network intrusions compromise the privacy of an individual because the data resides on the victim's network.
? Access Device Fraud (18 U.S.C. § 1029) - The term "access device" includes passwords, electronic banking account numbers, and credit card numbers. It can also be any card, serial number, or personal identification number.
? CAN-SPAM Act (18 U.S.C. § 1037) - provides a means for prosecuting those responsible for sending large amounts of unsolicited commercial email (a.k.a. "spam").
? Wire Fraud (18 U.S.C. § 1343) - pertains to fraud committed by means of fax, telex, modem, and Internet transmissions.
? Communication Interference (18 U.S.C. § 1362) - provides a means for prosecuting anyone who injures or destroys any of the works, property, or material of any radio, telegraph, telephone or cable, line, station, or system, or other means of communication, operated or controlled by the United States, or used or intended to be used for military or civil defense fun