**John Deutch**
**Director of U.S. Central Intelligence**

**Senate Governmental Affairs Committee**
**Permanent Subcommittee on Investigations**
**25 June 1996**

I wish to thank you for inviting me to appear before you this morning and speak about foreign information warfare activities against the United States. Protecting our critical information systems and information-based infrastructures is a subject that is worthy of considerable attention and is an issue that I am deeply concerned about.

Over the past 20 years, our nation has witnessed and contributed greatly to a technology revolution. As a result, our government, business, and citizens have become increasingly dependent on an interconnected network of telecommunications and computer-based information systems. These systems, such as the ones comprising the public switched telephone network, serve as a critical backbone for the entire U.S. public and private sectors. U.S. military logistic and operational elements increasingly rely on computer databases and the public telephone network for their classified, as well as unclassified, activities. In addition, the U.S. civil sector also increasingly depends on the uninterrupted and trusted flow of digital information. Day-to-day operations of U.S. banking, energy distribution, air traffic control, emergency medical services, transportation, and many other industries all depend on reliable telecommunications and an increasingly complex network of computers, information databases, and computer-driven control systems. The Internet has created a global information network that will be an enabler for an exciting new opportunity for digital commerce. This connectivity will create a seemingly seamless world of commerce without borders.

I, like many others in this room, am concerned that this connectivity and dependency make us vulnerable to a variety of information warfare attacks. While attention is focused on computer-based "cyber" attacks, we should not forget that key nodes and facilities that house critical systems and handle the flow of digital data can also be attacked with conventional, highexplosives. These information attacks, in whatever form, could not only disrupt our daily lives, but also seriously jeopardize our national or economic security. Without sufficient planning as we build these systems, I am also concerned that the potential for damage could grow in the years ahead.

I welcome the efforts of this subcommittee to increase public awareness about these important issues. I believe steps need to be taken to address information system

vulnerabilities and efforts to exploit them. We must think carefully about the kinds of attackers that might use information warfare techniques, their targets, objectives, and methods.

There has been much discussion in the press and testimony before this subcommittee about computer-based intrusions into banks and other financial institutions. We are keenly aware of the several, well-publicized incidents where computers were used to divert funds by false bank wires, embezzlement, and credit card fraud. To date, these incidents appear to be isolated and the goal limited to theft; that is, high-technology bank robbery. If so, they do not yet pose a serious national security threat to the United States. However, the number and size of these intrusions may grow to the point where they begin to threaten our economic well-being. In addition, we do not fully understand the real source and purpose of these events. Some may be sponsored by foreign adversaries in support of broader political, economic, or military goals.

My greatest concern is that hackers, terrorist organizations, or other nations might use information warfare techniques as part of a coordinated attack designed to seriously disrupt:

-- infrastructures such as electric power distribution, air traffic control, or financial sectors;

-- international commerce; and

-- deployed military forces in time of peace or war.

Virtually any "bad actor" can acquire the hardware and software needed to attack some of our critical information-based infrastructures. Hacker tools are readily available on the Internet, and hackers themselves are a source of expertise for any nation or foreign terrorist organization that is interested in developing an information warfare capability. In fact, hackers, with or without their full knowledge, may be supplying advice and expertise to rogue states such as Iran and Libya.

It is important to keep in mind, however, that computer-based tools are only one part of an information warfare capability. An adversary also needs highly detailed information about the target and its vulnerabilities, access to the target, and some way to judge how effective the attack will be. While some key U.S. infrastructure targets may be vulnerable to both physical destruction and "cyber" attacks, others are more secure.

Last summer, the National Intelligence council, with help from a number of Intelligence Community agencies, produced a classified report compiling our

knowledge of foreign information warfare plans and programs. Produced at the request of the Pentagon, it focused on foreign efforts to attack the U.S. public switched telephone network and so-called Supervisory Control and Data Acquisition (or SCADA) systems -- the computers that control electric power distribution, oil refineries, and other similar utilities. This Intelligence Community publication was the first of its kind on this topic and served as a vehicle for organizing the Intelligence Community's collection and analysis on this subject.

While the details are classified and cannot be discussed here, we have evidence that a number of countries around the world are developing the doctrine, strategies, and tools to conduct information attacks. At present, most of these efforts are limited to information dominance on the battlefield; that is, crippling an enemy's military command and control centers, or disabling an air defense network prior to launching an air attack. However, I am convinced that there is a growing awareness around the world that advanced societies, especially the United States, are increasingly dependent on open, and potentially vulnerable information systems.

The Intelligence Community is on the look-out for information that would indicate whether any of the "rogue" states have plans and programs underway to develop an offensive information warfare capability. These countries are very difficult intelligence targets and such programs, by their nature, are almost certainly highly covert and difficult to uncover. In virtually all of them we see advances in computer connectivity and information systems technology that would contribute to an offensive capability. We are alert for any evidence that these technologies are being applied to offensive information warfare programs, as well as information that suggests they may be sponsoring hacker activities.

International terrorist groups clearly have the capability to attack the information infrastructure of the United States, even if they use relatively simple means. Since the possibilities for attacks are not difficult to imagine, I am concerned about the potential for such attacks in the future. The methods used could range from such traditional terrorist methods as a vehicle-delivered bomb -- directed in this instance against, say, a telephone switching center or other communications node -- to electronic means of attack. The latter methods could rely on paid hackers. The ability to launch an attack, however, are likely to be within the capabilities of a number of terrorist groups, which themselves have increasingly used the Internet and other modern means for their own communications. The groups concerned include such well-known, long-established organizations as the Lebanese Hizballah, as well as nameless and less well-known cells of international terrorists such as those who attacked the World Trade Center.

As I noted earlier, many of the tools and technologies needed to penetrate computer systems and launch information warfare attacks are readily available to foreign

adversaries. However, we need to remember that a threat is comprised not only of a capability, but also the intent to conduct an attack.

There are a number of activities underway designed to improve our ability to quantify the information system threat to our critical information systems.

-- First, we have initiated new collection activities designed to uncover evidence of foreign intent to attack our systems. Some of these initiatives involve traditional intelligence resources such as HUMINT and SIGINT. Unfortunately, obtaining additional information on foreign information warfare plans and programs will take some time.

-- Second, we are working closely with the FBI and Department of Justice on this issue. I recognize that information warfare threat analysis is a non-traditional intelligence problem requiring non-traditional sources of data. One effort looks for foreign sponsorship of U.S.-based computer hacking activities as well as for evidence of organized crime involvement.

-- Third, both the law enforcement and Intelligence Communities are attempting to forge working relationships with the private sector, including U.S. corporations and academic institutions. As we all know, the private sector is being "hit" every day by hackers. I believe that foreign organized crime is behind some of these events and we are eliciting the private sector's help in looking for evidence of foreign involvement and sponsorship. However, obtaining computer intrusion data from U.S. banks, telecommunications companies, and other institutions has been difficult. Although the situation is improving, many of these firms are still reluctant to share information on intrusions for fear of losing consumer confidence. I know the subcommittee witnessed this problem first-hand several weeks ago at your last hearing. We are working hard to develop a relationship with industry based on trust and confidentiality.

-- Fourth, the intelligence agencies are devoting additional resources to information system threat analysis. For example, analysts at CIA are developing methods to assess the status of foreign information warfare programs. At DIA, analysts are working on ways to understand the warning indicators signaling that a major information warfare attack against the United States is planned or imminent.

-- Fifth, in order to provide an increased Intelligence Community information warfare focus, the deputy secretary of defense and I are looking to reorganize existing efforts and create a new center at the National Security Agency.

-- Finally, the National Intelligence Council is preparing a National Intelligence Estimate on this subject. This NIE will build on their report produced last summer and

cover many of the topics I have discussed this morning. Participants include not only the various intelligence agencies, but also the FBI, DISA, the military services computer crime units, and government representatives with liaison responsibility to the major telecommunications providers. I have directed the National Intelligence Council to complete this effort by 1 December.

I am convinced that organized information warfare threat from both state and non-state actors will grow over the next decade as the technology proliferates. I am encouraged by the steps we have taken over the past year to improve our collection and analytic posture on this issue.

However, intelligence and threat analysis are only part of the infrastructure protection process. We also need to determine which systems are most important for the functioning of our society and which are most vulnerable to attack. The steps outlined by Attorney General Reno in the Critical Infrastructure Security study, in which the Intelligence Community participated, is an excellent starting point for government action. Much more needs to be done. I look forward to working with this subcommittee and others on this issue in the months ahead.