Testimony of Richard A. Clarke

before the

COMMITTEE ON GOVERNMENT REFORM

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

April 8, 2003

"MAJOR CYBERSPACE VULNERABILITIES WILL BE USED AGAINST US"

Mr. Chairman,

It is a pleasure to testify before your committee today, the first time I have testified before any Congressional committee since leaving the Federal service several weeks ago after thirty years.

Before I begin, however, I would like to pay tribute to Chairman Putnam, both for calling this hearing and for his keen interest in the security of the United States. Almost no one knows that when Congressman Putnam first came to the House, before the events of September 11th, he sought out a Special Assistant to the President for a briefing on the threats posed by al Qida at a time when many in Congress and most people in America did not know what al Qida was.

It is not surprising to me, therefore, that you are now focusing on Cyber Security, Mr. Chairman. Once again, you are seeking to understand the emerging threats to our country before they can damage us.

The Threat and the Vulnerabilities

Let me begin by talking a little bit about the threat and the vulnerabilities.

For many, the cyber threat is hard to understand. They think that these cyber attacks are unfortunate, but are just a cost of doing business, just a minor nuisance in a multi-trillion dollar economy. No one has died in a cyber attack, after all, there has never been a smoking ruin for cameras to see.

Such reasoning is dangerous. Implicit in such thinking is the unarticulated notion that the only cyber attacks that can happen in the future are those similar to what has happened in the past. Implicit is the 20th century notion that if it is not a smoldering heap with a body count, there has been no real damage.

That is the kind of thinking that said prior to September 11th that the only kind of hijacking we will ever have in the US would be the flights to Havana we had in the past. It is the kind of thinking that said we never had a major foreign terrorist attack in the United States, so we never would; Al Qida has just been a nuisance, so it never will be more than that.

The threat is really very easy to understand. If there are major vulnerabilities in the digital networks that make our country run, then someday, somebody will exploit them in a major way doing great damage to the economy. What could happen? Transportation systems could grind to a halt. Electric power and natural gas systems could malfunction. Manufacturing could freeze. 911 emergency call centers could jam. Stock, bond, futures, and banking transactions could be jumbled. If that major attack comes at a time when we are at war, it could put our forces at great risk by having their logistics system fail.

Meanwhile, short of the Big Attack, there is damage being done every day. The threat ranges from minor cyber vandalism to theft of intellectual property and personal identity, to extortion, industrial espionage, international spying, to stoppages of sales or production. The culprits range from cyber joy riders, to thieves, to organized criminals, to corporate spies, to terrorist groups, to nation states.

Several nation states, including our own, have formed intelligence and military units to exploit cyber vulnerabilities for information collection and for damaging enemies' infrastructure in future wars. They all must think there is some potential for doing serious damage to an enemy not with bombs and bullets but with bits and bytes.

.

I am not alone in thinking there is a serious cyber threat. Who is convinced that the threat is real and important to our national economy and national security? In 1997 a Presidential Commission of distinguished leaders concluded there was an urgent threat. A National Academy of Sciences panel reached the same conclusion. A Presidential Decision Directive and National Plan followed. Then in the Bush Administration, the President signed an Executive Order and a National Strategy on cyber security. President Bush requested an increase of 64% in cyber security spending to defend federal departments' systems in his first budget. The Congress approved it and added its own Cyber Security Research Act. The House of Representatives recently formed a Cyber Security sub-committee.

In the private sector, while spending is down, IT security spending is up. Companies are buying software and hardware to find and fix their vulnerabilities. Segments of the private sector have united to form groups to share information about cyber security and to develop best practices to prevent and recover from cyber attacks.

Every few weeks brings further evidence that there are significant vulnerabilities in our national cyber infrastructure.

In January, someone wrote a little piece of computer code. It was a simple enough task. They took a glitch in Microsoft's SQL Server software that Microsoft had warned about months before and for which Microsoft had provided a fix. Then the hacker added a couple of lines of code that would cause their little program to search the internet for systems that had not applied the fix. When the program found such "unpatched" systems, the code would use the glitch to enter the vulnerable computer, destroy files, and use the infected computer as a launch point to attack any other computer it could find.

Then the hacker hit “send.”

Fifteen minutes later, over 300,000 computers were crashing. Some bank ATM machines went off line. Some routers that run computer networks flapped and were unable to send internet traffic. Some 911 call systems were hit. An airline cancelled flights. Some companies, unable to work, sent employees home. Untold millions of dollars were spent cleaning it up.

That was all the work of one hacker, exploiting a vulnerability in one company’s server software that had been known for months, and which most systems administrators had fixed. But because of the high degree of interconnectedness and interdependency in cyberspace, systems in addition to servers crashed, companies that had fixed the vulnerability were hit anyway, and companies that were not even running the software were damaged.

That attack was not hard to write. And it was just one of many such attacks that have been tried in the last few years.

The vulnerability that was exploited was just one of the 2800 glitches in software that have been publicly revealed.

In addition to the January worm I discussed called “sapphire” recent months have seen the first concerted attack on the mechanisms of the internet itself, the Domain Name System servers. We have also seen the discovery of a major flaw in “Send Mail” a system used widely in government and industry.

They are just the tip of the iceberg.

People who ask "who is the threat" are to some extent missing the point. As long as there are major vulnerabilities in our cyber infrastructure, and there are many, some one will exploit them. We can not anticipate and stop every threat. We can, however, start systematically to eliminate the vulnerabilities they could exploit.

What is to be Done?

Mr. Chairman, the President issued a *National Strategy to Secure Cyberspace* in February. It was the work of thousands of Americans from all sectors of our economy. It was developed with 10 White House Town Hall meetings held around the country. A first draft of the Strategy was posted for all America to review and comment upon.

The five National Priorities and the numerous specific steps under each of those priorities are a road map for government partnership with the private sector to begin eliminating the cyber vulnerabilities.

I want to highlight ten specific steps, which I believe deserve immediate attention of the House and of this Committee.

First, the Department of Homeland Security must organize itself and recruit the personnel necessary to carry out its significant responsibilities under the President's approved Strategy. Three of the five priorities in the strategy call upon DHS to take the lead. To date, DHS has not formed a National Cyber Security Center to be the focal point for its responsibilities in this area. Nor have they recruited a cadre of nationally recognized cyber security experts. They are not currently in position to carry out their responsibilities under the President's *National Strategy*.

Second, the U.S. Government must have a Chief Information Security Officer to insure that the Federal departments secure their systems. That CISO must have executive authority to direct action by agencies. Without such an official departments will continue as they have for years, vulnerable to cyber intrusion and woefully behind in the deployment of modern IT security technology. To date OMB has attempted to perform this function with one or two people buried in their bureaucracy and an interagency committee of the CIO Council, which lacks both expertise and authority.

Third, the Congress should appropriate the funds authorized by the Cyber Security Research Act, even if the Administration does not seek the full authorization. In doing so, the Congress should front end load the multi-year $900 million with three year programs. Funds should not go to universities alone, as is the tradition with the National Science Foundation, but should be made available to the Federally Funded research and Development Centers and National Labs such as MITRE, Los Alamos, and Livermore.

Fourth, Congress should direct the implementation of a program to secure the mechanisms of the internet that are owned in common, specifically the Domain Name System (DNS) and the Border Gateway Protocol (BGP). These two systems are extremely vulnerable today and their destruction or damage could halt the internet and all associated networks.

Fifth, Congress should direct and fund the GAO to install vulnerability scanning sensors in all Federal departments' networks. Such sensors are available commercially are work well. These sensors could report daily, weekly, or monthly on which of the 2800 known vulnerabilities are present in each network. With this knowledge, the departments could eliminate the vulnerabilities. The reports of the sensors should be given to this Committee, to the Inspector Generals of the Departments so that they can carry out their legal responsibilities with regard to cyber security, to the department CIOs, and to the Department leadership.

Sixth, this Committee should direct the expansion of the Patch Management System recently created by GSA. Over 90% of detected intrusions utilize known vulnerabilities for which a fix or "patch" had already been made publicly available. The GSA Patch system makes these fixes freely available to departments on a voluntary basis. The new system should be expanded to identify when the patches have been applied (and when they have not been) and to identify in advance potential conflicts between the patching software and other widely utilized software. Expanding this program is the most cost effective expenditure that this Committee could direct.

Seventh, this Committee should require that all Federally employees utilize a Common Access Card similar to the DOD "CAC" program to log on to their computers. The CAC is a multi-factor authentication device that can replace vulnerable passwords and can permit encryption. DOD has proved it can work.

Eighth, this Committee should communicate to the Executive Branch agencies its support for increased out sourcing of IT security to Managed Security Providers (MSPs). We kid ourselves, Mr. Chairman, if we believe that most departments can operate 24 x 7 command centers to monitor intrusion detection devices and firewalls. Moreover, these systems constantly alarm and only trained experts with a synoptic view over a wide range of networks can tell the wheat from the chaff.

Ninth, the Congress should support the expansion of private sector Cyber Security Best Practices, Information Sharing, and Cyber Security Risk Management Insurance. These three elements are essential to the success of a voluntary, non-regulatory approach to private sector cyber security. To do so, Congress should, inter alia, hold oversight hearings into the

implementation of the voluntary guidelines and Best Practices developed by the FCC's National Interoperability and Reliability Council (NIRC) for Internet Service Providers (ISPs). Congress should consider cost sharing with the Information Sharing and Analysis Centers (ISACs) formed by industry groups. The Terrorism Risk Insurance Act should be examined for the role that in can play in encouraging the insurance industry to underwrite cyber security risk policies, based on Best Practices.

Finally, Mr. Chairman, the Congress should require every department to operate a Cyber Security Awareness program to train employees on the risks of poor IT security and the steps they can each take to help secure the networks. Many Federal employees do not know when they are placing their department's network at risk by their own practices. Boring lectures and employee handbooks will not suffice. Departments should employ Learning /Teaching Computer Games, contests, and other innovative techniques.

These ten steps alone are not sufficient, but they are within the power of this Committee or this Congress, and they would be a very good start. Thank you again for the opportunity to testify before this Committee.