



United States
of America

Congressional Record

PROCEEDINGS AND DEBATES OF THE 110th CONGRESS, FIRST SESSION

Vol. 153

WASHINGTON, MONDAY, SEPTEMBER 10, 2007

No. 133

House of Representatives

The House met at 10:30 a.m. and was called to order by the Speaker pro tempore (Mrs. TAUSCHER).

DESIGNATION OF THE SPEAKER PRO TEMPORE

The SPEAKER pro tempore laid before the House the following communication from the Speaker:

WASHINGTON, DC,
September 10, 2007.

I hereby appoint the Honorable ELLEN O. TAUSCHER to act as Speaker pro tempore on this day.

NANCY PELOSI,
Speaker of the House of Representatives.

MORNING-HOUR DEBATE

The SPEAKER pro tempore. Pursuant to the order of the House of January 4, 2007, the Chair will now recognize Members from lists submitted by the majority and minority leaders for morning-hour debate. The Chair will alternate recognition between the parties, with each party limited to not to exceed 30 minutes, and each Member, except the majority leader, the minority leader, or the minority whip, limited to not to exceed 5 minutes.

The Chair recognizes the gentleman from Florida (Mr. STEARNS) for 5 minutes.

CHINESE CYBER SPIES—AN EMERGING THREAT

Mr. STEARNS. Madam Speaker, my colleagues, the control of information is critical to national security. This asset was compromised as reported in the London Times AP story in the Washington Post recently, last week. It was compromised from a cyber attack against the Department of Defense's unclassified e-mail system, which included the e-mail accounts of Defense Secretary Robert Gates. While the Pentagon does not have sufficient

proof to formally make an accusation, China is the prime suspect. The responsibility is unclear, because China is home to many insecure computers and networks that hackers in other computers could use to simply disguise their locations and launch these attacks, making proper attribution difficult.

The Chinese Government replied, "It has always opposed any Internet wrecking crime, including hacking, and crack down on it according to their law." This is not true. Last June was not the first cyber attack that points back towards China. In 2005, a group with ties to China compromised secure networks from the Redstone Arsenal Military Base, to NASA, to the World Bank. In one case, the hackers stole flight planning software from the Army. The files they have obtained are not classified, but many are strategically important enough to require U.S. Government licenses for foreign use.

Experts note China's military has openly discussed using cyber attacks as a means of defeating a more powerful conventional military such as ours. In fact, other governments have also been the targets of these vicious cyber attacks. Unidentified officials in Germany and Britain reported to the media that government and military networks had been broken into by hackers backed by the Chinese Army. The Guardian reported that Chinese attackers launched online assaults on the network in Britain's Parliament, the Foreign Office, and Defense Ministry. My colleagues, last month the German weekly Der Spiegel also reported that computers at the chancellery and three ministries had been infected with so-called Trojan horse programs, which allowed an attacker to spy on information in those computers. The report, which appears on the eve of German Chancellor Merkel's visit to Beijing, said Germany's domestic intelligence agency believed hack-

ers associated with the Chinese Army might have been behind the attacks. Motives for such hacking may range from the stealing of secrets or confidential technology to probing for system weaknesses and placing hidden viruses that could be activated in case of a conflict.

The reported Pentagon attack was the most flagrant and brazen to date, said Alex Neill, an expert on the Chinese military at London's Royal United Services Institute. Quoted by the British newspaper, The Guardian, Neill said such attacks begin at least 4 years ago, and are increasing at an alarming rate.

Now, this is a substantial threat to the security of the United States and its allies. In January 2005, Japanese officials had reported that Chinese hackers were routinely attacking web sites and Internet services. According to the Korean Information Security Agency, a total of 10,628 cases of hacking were reported in the first half of the year 2004, 30 times higher than for the same period in 2003. In 2005, Chinese hackers assaulted South Korean government computers, gaining access to information concerning the country's National Assembly, Atomic Energy Research Institute, Democratic Progressive Party, and even the itinerary of the South Korean president himself.

Whether or not cyber attacks are government sponsored, China has become a growing focus of global antihacking efforts. In a report earlier this year, security software maker Symantec Corporation listed China as having the world's second largest amount of computer activity. Experts say the attacks originating in China often employ standard weaponry such as Trojan horses and worms, and many other sophisticated techniques. In some cases, hackers slip in after launching viruses to distract monitors, or coordinate multiple attacks for

This symbol represents the time of day during the House proceedings, e.g., 1407 is 2:07 p.m.

Matter set in this typeface indicates words inserted or appended, rather than spoken, by a Member of the House on the floor.



Printed on recycled paper.

H10323