The threat to U.S.-based computer networks is one of the country's most pressing security problems, and Congress needs to act on it soon, the director of national intelligence told a congressional panel today.

James R. Clapper Jr. said he and all of the U.S. intelligence leadership agree the United States is in a type of cyber Cold War, losing some $300 billion annually to cyber-based corporate espionage, and sustaining daily intrusions against public systems controlling everything from major defense weapons systems and public air traffic to electricity and banking.

Clapper was joined by CIA Director David H. Petraeus, Defense Intelligence Agency Director Army Lt. Gen. Ronald L. Burgess Jr. and FBI Director Robert S. Mueller for a House Select Intelligence Committee hearing on worldwide threats. He urged lawmakers to pass a bill that forces intelligence sharing between the government and the private sector, such as the Defense Industrial Base pilot program that then-Deputy Defense Secretary William J. Lynn III launched last year.

"It's clear from all that we've said and I hope predications about mass attacks don't become a self-fulfilling prophesy but we all recognize we need to do something," he said.

Clapper also urged Congress to reauthorize the Foreign Intelligence Surveillance Act, which he called crucial to intelligence gathering. It expires this year.

The director said he foresees a cyber environment in which technologies continue to be fielded before effective security can be put in place. Among the greatest challenges in cyber security, he added, are knowing the perpetrator of a cyber attack in real time and capabilities gaps in the cyber supply chain the entire set of key actors involved in the cyber infrastructure.

Mueller noted that the National Cyber Task Force includes 20 U.S. agencies, "so when a major

intrusion happens, we're all at the table." The "breaking down of stovepipes" and sharing information in cyber security "is as important now as it was before 9/11," he added.

The FBI director told the panel that 47 states have different reporting requirements for cyber attacks, and the private sector doesn't have to report them at all. "If they're not reported, we can't prevent the next one from happening," he said.

Mueller said the cyber threat is growing and is important to address. "I do believe cyber threats will equal or surpass the threat from terrorism in the near future," he said.

Clapper agreed. "We all recognize this as a profound threat to this country, to its future, to its economy, to its very being," he said. "We all recognize it, and we are committed to doing our best in defending the country."