FBI ranks cyber attacks third most dangerous behind nuclear war and WMDs

Contributed by Rick C. Hodgin
Wednesday, January 07, 2009 00:01

Yesterday, the FBI announced it considers cyber attacks to be the third greatest threat to the security of the United States. The only two preceding it are nuclear war and weapons of mass destruction (WMD).

Washington (DC) - Yesterday, the FBI announced it considers cyber attacks to be the third greatest threat to the security of the United States. The only two preceding it are nuclear war and weapons of mass destruction (WMD).

A new term "Cybergeddon" has been coined, relating to the potential loss of intellectual property, intelligence infrastructure and related industries dealing primarily in data exchange or storage. The target today is not a person or place, but rather a person's data or a place's significance.

Shawn Henry, assistant director of FBI's cyber division, said terrorists are attempting to create a type of "virtual 9/11" by "inflicting the same kind of damage on our country, on all our countries, on all our networks, as they did in 2001 by flying planes into buildings." Though, he indicates, this time the damage will come without commensurate levels of visible destruction.

While the United States has, to date, never seen an attack of that scale, Russian hackers allegedly mounted similar Internet attacks on networks in Estonia and Georgia last year. And most recently, several Israeli websites have been attacked just within the last few days.

Donald Codling, the FBI's cyber unit liaison with the Department of Homeland Security, said, "It used to be we'd chase people around, literally carrying duffel bags of cash. Nowadays the guy can use his SIM chip and he can move money all over the world and his confederates can withdraw that money from an ATM in a currency of his or her choice. It's extraordinarily difficult for us to catch them."

Christopher Painter, an FBI "specialist," described the basic weakness in fighting for cyber security. He said the threat is largely invisible and people don't always take it seriously. "It's not like a fire. It's hard to get your head around the threat. We often discover a company has been attacked and we tell them that and they don't know."