Computer expert says US behind Stuxnet worm

3 March 2011, by Glenn Chapman

An Iranian youth browses at an Internet cafe in the city of Hamadan in 2009. A German computer security expert said Thursday he believes the United States and Israel's Mossad unleashed the malicious Stuxnet worm on Iran's nuclear program.

A German computer security expert said Thursday he believes the United States and Israel's Mossad unleashed the malicious Stuxnet worm on Iran's nuclear program.

"My opinion is that the Mossad is involved," Ralph Langner said while discussing his in-depth Stuxnet analysis at a prestigious TED conference in the Southern California city of Long Beach.

"But, the leading source is not Israel... There is only one leading source, and that is the United States."

There has been widespread speculation Israel was behind the Stuxnet worm that has attacked computers in Iran, and Tehran has blamed the Jewish state and the United States for the killing of two nuclear scientists in November and January.

"The idea behind Stuxnet computer worm is really quite simple," Langner said. "We don't want Iran to get the bomb."

The malicious code was crafted to stealthily take control of valves and rotors at an Iranian nuclear plant, according to Langner.

"It was engineered by people who obviously had inside information," he explained. "They probably also knew the shoe size of the operator."

Stuxnet targets computer control systems made by German industrial giant Siemens and commonly used to manage water supplies, oil rigs, power plants and other critical infrastructure.

"The idea here is to circumvent digital data systems, so the human operator could not get there fast enough," Langner said.

"When digital safety systems are compromised, really bad things can happen -- your plant can blow up.

Most Stuxnet infections have been discovered in Iran, giving rise to speculation it was intended to sabotage nuclear facilities there. The worm was crafted to recognize the system it was to attack.

The New York Times reported in January that US and Israeli intelligence services collaborated to develop the computer worm to sabotage Iran's efforts to make a nuclear bomb.

Russia called on NATO in January to launch an investigation into the computer worm that targeted a Russian-built Iranian nuclear power plant, saying the incident could have triggered a new Chernobyl.

Russia's envoy to NATO in January said Stuxnet caused centrifuges producing enriched uranium at the Bushehr plant to spin out of control, which could have sparked a new "Chernobyl tragedy," the 1986 nuclear meltdown in Ukraine.

"The operators saw on their screens that the centrifuges were working normally when in fact they

were out of control," Dmitry Rogozin told reporters after meeting with ambassadors from the 28-nation Western alliance.

Russia is helping Iran build a nuclear power plant in the southern city of Bushehr for civilian use.

Langner said the Stuxnet code was designed to trick human operators by showing them recorded readings indicating machinery is running normally while behind the scenes they are heading for destruction.

"It's definitely hard-core sabotage," Langner said of Stuxnet. "It's like in the movies where during a heist the security camera is running pre-recorded video showing nothing is wrong."

Iran's envoy to the International Atomic Energy Agency has denied that the Stuxnet attack effected the country's nuclear program, including Bushehr.

A terrifying aspect of Stuxnet, according to Langner, is that it is a generic attack that would work well in factories, power plants, or other operations plentiful in the United States.

"It's a cyber weapon of mass destruction," Langner said. "We'd better start preparing right now."