Today's threat: Computer network terrorism

January 19 2010

According to Dr. Levyatan, in today's world, the battlefield is not only comprised of tanks and planes, but also computer experts' and hackers' keyboards. To date, most of the 'online fighting' has focused on attempts to vandalize and immobilize leading websites to impose a virtual presence and damage morale. The next stage is the attempt to cause damage to systems that are operated by computer networks, such as financial systems, power stations, hospitals, television broadcasts and satellites.

"A fleet of fighter planes is not necessary to attack a power station; a keyboard is sufficient. And if you don't have the skills, there are enough mercenary hackers who can do it for you," says Dr. Yaniv Levyatan, a University of Haifa expert on information warfare.

"Carry out all my demands or the entire country's electricity will be cut off." Is this another line from a suspense film, or is it a palpable threat made possible with a computer keyboard? " Today, there is a growing trend amongst hackers around the world to threaten national infrastructures for ransom," says Dr. Yaniv Levyatan, an expert in information war at the University of Haifa.

If someone still thinks that this is science fiction, Dr. Levyatan notes how just recently, in November 2009, Brazil's electricity was blacked out for more than an hour. "It is still not clear what happened, but one assumption is that it was a cyber -terror attack," he suggests, adding that in 2007 Estonia's computer infrastructures were attacked, most likely by Russian hackers, bringing the country to a near standstill for about 48 hours.

According to Dr. Levyatan, in today's world, the battlefield is not only comprised of tanks and planes, but also computer experts' and hackers' keyboards. "To date, most of the 'online fighting' has focused on attempts to vandalize and immobilize leading websites to impose a virtual presence and damage morale. For example, during the Second Lebanon War, Israeli and Hezbollah-supporting hackers were at "war" as each side attempted to damage and immobilize each other's websites. Likewise, during Operation Cast Lead in Gaza, many Israeli websites were attacked by Hamas-supporting hackers.

The next stage is the attempt to cause damage to systems that are operated by computer networks, such as financial systems, power stations, hospitals, television broadcasts, and satellites. "A fleet of fighter planes is not necessary to attack a power station; a keyboard is sufficient. And if you don't have the skills, there are enough mercenary hackers who can do it for you," says Dr. Yaniv Levyatan.

Provided by University of Haifa

Citation: Today's threat: Computer network terrorism (2010, January 19) retrieved 11 July 2024 from https://phys.org/news/2010-01-today-threat-network-terrorism.html