Cyber attacks on Gulf infrastructure seen rising

Mahmoud Habboush, Reuters

(Reuters) - The former chief of the United Arab Emirates' air force said his country's advanced cyber infrastructure made it a favorite target for hackers, especially when tension heightened in the Israeli-Palestinian conflict.

"The last war in Gaza led to a barrage of cyber attacks because UAE has advanced telecommunications infrastructure," retired Major General Khaled al-Buainnain said.

"The biggest attack was during the 2006 Israel-Lebanon war which was carried out by pro-Israeli hackers who did not understand the nature of the conflict and its parties."

His comments came a few months after a virus infected 30,000 computers [1] at Saudi Arabia's national oil company, Saudi Aramco, which said on Sunday the attack was aimed at stopping oil and gas production at the world's biggest oil exporter.

The attack failed to disrupt production, but was one of the most destructive cyber strikes against a single business [2].

Cyber attacks on infrastructure by hostile governments, militant groups or private "hacktivists" have the potential to disrupt oil and gas supplies to power plants and desalination plants, on which the Gulf states are heavily reliant.

"There is an interest at the political level in cyber security which has prompted investments in protection systems to protect the interest of the people, the government and national security," Buainnain said, speaking on the sidelines of a cyber security conference in Dubai.

"All the evidence that we have confirms that the attacks will increase," said Robert Eastman, vice president for global solutions at Lockheed Martin.

Eastman said Lockheed Martin, the Pentagon's top supplier, was in discussions with officials in Qatar, Saudi Arabia [3] and the United Arab Emirates about the company's training and vulnerability analysis systems.

A company official estimated last month that 5 to 8 percent of Lockheed's revenues in the information systems sector were related to cyber security. Lockheed generated $9.4 billion sales in that division in 2011.

CYBER RISKS

"All companies have to prepare response plans," said Hervi Meurie, general manager of C4 Advanced Solutions LLC, an Abu Dhabi-based technology and security firm. "What happens if the electricity network gets hit by a virus and goes

down for three days?"

Iran [4], the target of international economic sanctions focused on its oil industry over its disputed nuclear program, has been hit by several cyber attacks in the last few years.

In April, a virus targeted Iranian oil ministry and national oil company networks, forcing Iran [5] to disconnect the control systems of oil facilities including Kharg Island, which handles most of the country's crude exports.

Iran has blamed some of the attacks on the United States, Israel and Britain; current and former U.S. officials told Reuters this year that the United States built the complex Stuxnet computer worm to try to prevent Tehran from completing suspected nuclear weapons work.

Buainnain said he believed Iran would remain the target of cyber attacks rather than a source for them.

"I don't think Iran poses any threat," he said. "I think their activity is less aggressive and more focused on intelligence gathering, they are in fact subject to cyber attacks because of the nuclear program."

He said the UAE was in the process of creating a government body that will be responsible for handling cyber threats, adding that the National Electronic Security Authority was expected to be officially launched within the next few months.

While it is standard industry practice to shield plant operating networks from hackers by running them on separate systems, these have not been enough to fend off cyber attacks.

Qatar's natural gas [6] firm Rasgas was hit by a cyber attack in September, although it has not said how much damage was caused or whether it was the same virus that hit Aramco.

Theodore Karasik, director of research at the Institute for Near East and Gulf Military Analysis which organized the conference, said governments and companies must stay on high alert.

"You're always in catch-up mode because the bad guys can out-think the good guys faster," he said. "The Gulf states need to stay as far ahead as possible given their enemies who may be more technically savvy."

(Writing by Mahmoud Habboush; Editing by Myra MacDonald)

Links:
[1] http://www.reuters.com/sectors/industries/overview?industryCode=104&lc=int_mb_1001
[2] http://www.reuters.com/finance?lc=int_mb_1001
[3] http://www.reuters.com/places/saudi-arabia
[4] http://www.reuters.com/places/iran
[5] http://www.reuters.com/places/iran?lc=int_mb_1001
[6] http://www.reuters.com/sectors/industries/overview?industryCode=185&lc=int_mb_1001