Power grid at risk from hackers: U.S.

Cyber-spies from Russia, China have penetrated system: report

By Steve Holland and Randall Mikkelsen, Reuters; With Files From News ServicesApril 9, 2009

The U.S. electricity supply is at "increasing" risk from computer hackers, Homeland Security Secretary Janet Napolitano said yesterday following reports cyber-spies from China and Russia have targeted the grid.

Experts fear stealth software has been placed in the system that could be used to disrupt networks at a time of war or crisis.

Ms. Napolitano said the power grid is vulnerable to potentially disabling computer attacks, while declining to comment on reports that an intrusion had taken place.

"The vulnerability is something that the Department of Homeland Security and the energy sector have known

about for years," she said. "We acknowledge that ... in this world, in an increasingly cyber-world, these are increasing risks."

Ms. Napolitano spoke after The Wall Street Journal reported that cyber-spies had penetrated the U. S. electrical grid and left behind software programs that could be used to disrupt the system.

The newspaper said the intruders have not sought to damage the power grid or other key infrastructure but could try during a crisis or war.

The United States for several years has accused the Chinese and Russians, among others, of using cyber-attacks to try to steal American trade, military and government secrets.

The Chinese have been particularly active, a former U. S. security official told Reuters.

"They are all over the place," said the official, who spoke on condition of anonymity. "They're getting into university systems, contractor systems, hacking government systems. There's no reason to think that the electrical system would be immune as well."

The U. S. Defence Department spent more than US$100-million in the past six months repairing various types of damage caused by cyber-attacks.

This week, General John Davis, the deputy commander of the joint task force for global operations, said cyber-attacks posed a serious and costly threat to government and commercial networks.

Eric Rosenbach, executive director for research at Harvard University's Kennedy School of Government's Belfer Center, said that if the latest reports were true, it showed that the Chinese and Russians were thinking strategically about how to either constrain the United States or inflict more damage if they ever felt they needed to do so.

"I think that China recognizes if, in a very strategic sense, you want to ensure you have the ability to exploit another country's potential weakness or vulnerability but do it in a way that isn't confrontational or cause an international crisis, then this is a very good way of doing that," he said.

The United States is not alone. CIA analyst Tom Donahue told a power-industry conference last year that "we have information from multiple regions outside the United States of cyber-intrusion into utilities followed by extortion demands."

The North American Electric Reliability Corp., the industry group with responsibility for grid reliability and security for the United States and Canada, said it was unaware of any cyber-attacks that have led to disruptions of electric service. The group has been working for several years with the industry to create and implement cyber-security measures.

Researchers at the University of Toronto recently revealed the presence of Ghost-Net, a global cyber-spying network run from China that has infiltrated 103 countries.

The research started as an investigation into interference with computers belonging to the Dalai Lama, the exiled Tibetan leader, and his supporters. It found that the Chinese had in many cases successfully searched computers, tapped into e-mails and turned on Web cameras and microphones to record conversations within range.