

# Cyber spies and thugs attacking power-water plants



by Glenn Chapman Fri Jan 29, 12:03 am ET

SAN FRANCISCO (AFP) – Power plants, oil refineries and water supplies increasingly dependent on the Internet are under relentless attack by cyber spies and thugs, according to a McAfee report.

The "Critical Infrastructure in the Age of Cyber-War" analysis by the US-based Center for Strategic and International Studies said the price of "downtime" from major attacks exceeds six million dollars a day.

"If cyberspace is the Wild West, the sheriff needs to get to Dodge City," concluded the study commissioned by McAfee, which sells computer security software.

In most developed countries, operating systems of critical infrastructure including power grids and oil refineries are linked to the Internet where they can be targeted for attacks.

"There are absolutely foreign entities that would definitely conduct (cyber) reconnaissance of our power infrastructure," said Michael Assante, chief security officer of the North American Electric Reliability Corporation.

"They would be looking to learn, get a foothold and try to maintain sustained access to computer networks."

Researchers surveyed 600 IT and security executives from critical infrastructure enterprises in 14 countries in September of 2009.

Operators of enterprises reported that their networks and control systems are under repeated cyberattack, according to the study.

And while defenses were deemed acceptable, harsh economic conditions have tightened spending on computer security while attackers have grown more sophisticated, survey results indicated. Related article: [Cyber arms race](#)

"There is no identifiable protection model that will keep pace with the evolution and sophistication of cyber threats," said Assante.

"In addition, innovative technologies, from cloud computing to Smart Grid meters and SCADA connectivity, continue to create new vulnerabilities."

While the most common target of attacks was financial information, operators of energy, oil, and gas facilities saw assaults on operational controls, according to the survey.

A third of the respondents saw the threat as growing, while two fifths said they expect a major Internet security incident in their sector within a year.

The United States said Thursday that Google's problems in China with cyberattacks could deter US companies from investing in the Asian economic powerhouse.

Google has threatened to abandon its Chinese search engine, and perhaps end all operations in the country over the recent cyberattacks. It has also said it is no longer willing to bow to Chinese government censors.

China has said the hacking charges were without foundation.

Critical systems operators feared the potential of cyber-war.

"Although attribution is always a challenge in cyberattacks, most owners and operators believe that foreign governments are already engaged in attacks on critical infrastructure in their country," the study said.

"Other cyberattackers range from individual hackers and e-vandals to organized crime enterprises. Financially motivated attacks like extortion and theft-of-service are widespread."

Oil and natural gas operations reported the highest rates of "stealth infiltration" with 71 percent claiming to have been targeted.

One-in-five critical infrastructure entities reported being the victim of extortion through cyberattack or threatened cyberattack within the past two years.

Extortion was described as demanding payment to appease attackers that say "hey, I can make the lights go out."

The study showed cyber-extortion to be most common in India, Saudi Arabia/Middle East, China and France.

China registered highest in infrastructure cyber-security while Italy, Spain and India were at the low end of the spectrum, according to the study.

"As long as major governments desire unimpeded operational freedom in cyberspace, it will continue to be the Wild West," researchers said.

"In the meantime, the owners and operators of the critical infrastructure which makes up this new battleground will continue to get caught in the cross-fire and may indeed need what amounts to their own ballistic missile defense."

---

Copyright © 2010 Yahoo! Inc. All rights reserved. [Questions or Comments](#) [Privacy Policy](#) [About Our Ads](#) [Terms of Service](#) [Copyright/IP Policy](#)