


HSDailyWire.com

THE BUSINESS OF HOMELAND SECURITY

[Home](#) [Transport / Border](#) [Biometrics](#) [Continuity / Recovery](#) [Infrastructure / IT](#) [Bloddefense](#) [Surveillance](#) [Detection](#) [Sci / Tech](#) [Markets](#) [Policy](#) [Energy](#) [Search](#)**China syndrome****Chinese hacking threatens U.S. critical infrastructure**

Published 2 June 2008

U.S. government networks, and the computer systems of U.S. and Western European companies, are under broad and systemic Chinese hacking campaign; in the case of private Western companies, China steals industrial secrets and patent information in order to hasten its rise to a position of global economic hegemony; in the case of U.S. critical infrastructure -- for example, control of electric power stations, several of which Chinese hackers have managed to disable -- China may be preparing for more sinister contingencies

As we have reported in several stories over the past few months, computer hackers in China, among them those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of U.S. companies and government agencies, stolen proprietary information from American executives in advance of their business meetings in China, and, in a few cases, gained access to the systems controlling U.S. critical infrastructure facilities. For example, Chinese hackers gained access to electric power plants in the United States, possibly triggering two recent and widespread blackouts in Florida and the Northeast, according to U.S. government officials and computer-security experts. One prominent expert [told](#) Shane Harris of the *National Journal* that he believes that China's People's Liberation Army played a role in the power outages. Tim Bennett, the former president of the Cyber Security Industry Alliance, a leading trade group, said that U.S. intelligence officials have told him that China's People's Liberation Army (PLA) in 2003 gained access to a network that controlled electric power systems serving the northeastern United States. The intelligence officials said that forensic analysis had confirmed the source, Bennett said. "They said that, with confidence, it had been traced back to the PLA." These officials believe that the intrusion may have precipitated the largest blackout in North American history, which occurred in August of that year. A 9,300-square-mile area, touching Michigan, Ohio, New York, and parts of Canada, lost power; an estimated 50 million people were affected.

Harris notes that, officially, the blackout was attributed to a variety of factors, none of which involved foreign intervention. Investigators blamed "overgrown trees" that came into contact with strained high-voltage lines near facilities in Ohio owned by FirstEnergy Corp. More than 100 power plants were shut down during the cascading failure. A computer virus, then in wide circulation, disrupted the communications lines that utility companies use to manage the power grid, and this exacerbated the problem. The blackout prompted President George Bush to address the nation the day it happened. Power was mostly restored within twenty-four hours. "There has never been an official U.S. government assertion of Chinese involvement in the outage," Harris writes, "but intelligence and other government officials contacted for this story did not explicitly rule out a Chinese role. One security analyst in the private sector with close ties to the intelligence community said that some senior intelligence officials believe that China played a role in the 2003 blackout that is still not fully understood. Bennett, whose former trade association includes some of the nation's largest computer-security companies and who has testified before Congress on the vulnerability of information networks, also said that a blackout in February, which affected three million customers in South Florida, was precipitated by a cyber-hacker. That outage cut off electricity along Florida's east coast, from Daytona Beach to Monroe County, and affected eight power-generating stations. Bennett said that the chief executive officer of a security firm that belonged to Bennett's trade group told him that federal officials had hired the CEO's company to investigate the blackout for evidence of a network intrusion, and to "reverse engineer" the incident to see if China had played a role.

Bennett, who now works as a private consultant, said he decided to speak publicly about these incidents to point out that security for the nation's critical electronic infrastructures remains intolerably weak and to emphasize that government and company officials haven't sufficiently acknowledged these vulnerabilities.

[About us](#) | [Subscribe](#) | [Advertise](#) | [Contact us](#) | ©2008 HS Daily Wire