Could cyberattacks knock out lights in the US? Not so easily

October 11 2017, by Matt O'brien

In this Nov. 12, 2015, file photo, a concrete pole carrying feeder lines stands outside an electric company substation in the U.S. Hackers likely linked to the North Korean government targeted U.S. electricity grid workers in September 2017, according to a security firm that says it detected and stopped the attacks, which didn't threaten any critical infrastructure. But the attempted breaches raise concerns. (AP Photo/Gerald Herbert, File)

Hackers likely linked to the North Korean government targeted a U.S.

electricity company last month, according to a security firm that says it detected and stopped the attacks.

John Hultquist, director of intelligence analysis for FireEye, said Wednesday that phishing emails were sent to executives on Sept. 22. The attacks didn't threaten critical infrastructure.

It's the latest example of cyberespionage targeting U.S. energy utilities, though experts say such attacks are often more about creating a psychological effect. It's easier to hack into a front-end computer system than tap into industrial controls.

Concerns about hackers causing blackouts have grown since cyberattacks in Ukraine temporarily crippled its power grid in 2015 and 2016. Such an attack would be harder to accomplish in the North America electricity grid because it's segmented by region.

Citation: Could cyberattacks knock out lights in the US? Not so easily (2017, October 11) retrieved 3 May 2024 from https://phys.org/news/2017-10-cyberattacks-easily.html