US Army must be prepared for cybersecurity threats to energy sector, study says

February 6 2014, by Jeff Falk

Cybersecurity threats to the United States' energy industry and infrastructure are rising and require increased preparedness by the U.S. Army and Department of Defense, according to a new paper from Rice University's Baker Institute for Public Policy.

The paper, "Hacks on Gas: Energy, Cybersecurity and U.S. Defense," was authored by Chris Bronk, a fellow in information technology policy at the Baker Institute and a former U.S. State Department diplomat who specializes in cybersecurity issues. Produced for the U.S. Army War College's Strategic Studies Institute, the paper considers potential cyberthreats relevant to the Army and Department of Defense's energy needs and purview, including the electrical grid, oil and gas security and the military's fuel supply chain, and proposes a range of policy and strategic recommendations the nation's military should undertake to address these threats.

"We should be concerned with cybersecurity in energy because, as with other areas of the global economy, computing has been widely adopted in the energy industry," Bronk said. "The Department of Defense is incredibly reliant on private sources of energy, and the level of preparedness for cyberattack among those sources likely varies greatly."

Bronk counts the 2012 "Shamoon" computer virus attack against national petroleum producer Saudi Arabian Oil Co. (also known as Saudi Aramco) as an example of the devastation that such attacks can cause. Shamoon reportedly spread across as many as 30,000 Windows-based

personal computers operating on the company's network. It may have taken Saudi Aramco almost two weeks to fully restore its network and recover from the disruption of its daily business operations caused by data loss and disabled workstations resulting from the incident.

Bronk said there are likely three major areas of energy-related cyber vulnerability that are relevant to the Army: the provision of electricity to bases and facilities by the electrical grid, both in the U.S. and abroad; the distribution of fuels to forces often operating some distance from major logistical hubs; and major cyberattacks against suppliers of fuels that would result in a significant disruption of supply or a rise in price.

"Other scenarios of attack are no doubt possible and are limited only by vulnerability, technical know-how and imagination," Bronk said. "Cyberattacks against Army logistics should be taken as a given, and a massive cyberattack against the oil and gas industry would be of great concern far beyond the Department of Defense."

Bronk proposed five immediate policy and strategic interventions the U.S. military should pursue to prepare for and manage cyberthreats to energy security:

Recognize that cyber incidents like safety or disruption events are not just organizational issues, but also issues of potential concern across an extensive, interconnected energy supply chain.

Develop trusted third-party and clearinghouse relationships aimed at developing better cyber intelligence and analysis.

Produce and constantly refine models of cyber risk intelligence, merging the valuation of assets/processes, threats and reasons for potential compromise.

Consider the cybersecurity ramifications as the Internet expands to cover more infrastructure, including hundreds of millions of energy-related computing devices.

Connect the spheres of geopolitics and the technical aspects of cybersecurity to develop holistic models for coping with the cybersecurity problem.

"These recommendations represent an initial thrust of activity, but instituting them will require difficult shifts in behavior for government and industry," Bronk concluded. "Deep analysis not only of vulnerability but also of the resiliency of the energy supply chain to a cyberattack is necessary."

More information: Read the full paper here: bakerinstitute.org/files/6195/download/

Provided by Rice University

Citation: US Army must be prepared for cybersecurity threats to energy sector, study says (2014, February 6) retrieved 26 April 2024 from https://phys.org/news/2014-02-army-cybersecurity-threats-energy-sector.html