Cybersecurity & Resiliency in the Electric Grid and Utility Critical Infrastructure

Harvard Kennedy School Energy Policy Seminar Series, Spring 2019

Monday, April 22, 2019

By Louisa Lund, Program Director, Consortium for Energy Policy Research

With respect to resilience, "A lot of what we have in the electric sector today comes from the impacts of weather events" according to Richard Mroz, Managing Director of Resolute Strategies and former New Jersey utility commissioner. Events like 2012's Superstorm Sandy, which impacted 71% of New Jersey's electric distribution system and resulted in five million New Jersey customers suffering an extended loss of power, prompted extensive state and federal efforts to improve communications, support mutual aid, ensure fuel availability, and establish institutions for better coordination within the electricity sector.

All of these efforts are relevant to cybersecurity resilience, but, at the same time, "Cybersecurity is like no other threat," Mroz said. It is impossible to predict a cybersecurity event in the same way you can predict a storm, for example. Moreover, the threat changes as the grid changes, for example with the increasing prevalence of two way power flows and with the development of the "internet of things," which has brought exponential growth of internet-connected devices and potential points of cybersecurity. Meanwhile, Mroz observed, common technology standards to govern these devices have yet to be developed.

New Jersey has taken the cybersecurity threat seriously, Mroz reported, adopting an "all hazards" approach, and directing all electric, gas, and water companies to establish cybersecurity plans. At the national level, efforts to plan for cybersecurity are growing, including national cybersecurity exercises and coordination work by numerous government agencies and NGOs, including Protect our Power, for which Mroz is a senior advisor.

Within this context, Mroz noted certain key issues that need additional work, including establishing a clearer inventory of best practices, above and beyond the minimal standards established by the North American Electric Reliability Corporation (NERC). Certain underserved systems—often small munis or rural power coops—may need additional support, Mroz noted. Additional planning is needed around how to ensure power can be restored if necessary—including the possibility of returning to more manual systems and consideration of the question of whether it is possible for the electric system to become over-digitized. Finally, qualified people in the area of cybersecurity are in great demand—keeping up with human resources needs is an ongoing challenge.

For public utility commissions, a key ongoing issue has to do with funding for utility cybersecurity efforts, Mroz said. In many states, statutes provide that public utility commissions may approve cost recovery only for those utility investments that can be shown to be "used and useful." It is not yet clearly established whether an investment made in anticipation of a potential threat that may never materialize can be considered to qualify for approval under this standard. "Innovative funding approaches may be necessary across states, if current regulations don't allow for funding," Mroz said.

Mroz spoke as part of the Kennedy School's Energy Policy Seminar Series, which is sponsored by the Consortium for Energy Policy Research of the Mossavar-Rahmani Center on Business and Government and by the Belfer Center for Science and International Affairs.