Roth: The Russians can’t take your microgrid

By Jim Roth, Director and Chair of the Firm’s Clean Energy Practice Group. This column was originally published in The Journal Record on March 26, 2018.

Jim Roth is a Director and Chair of the firm’s Clean Energy Practice.

Roth: The Russians can’t take your microgrid

On the list of benefits to increasing our use of renewable energy, safety is always one of them. Distributed generation, in particular, is more secure than our current energy infrastructure, and apparently Russia is out to prove it.

The situation we now face has been building. You might remember late last year when it was revealed that a National Security Agency contractor moved highly classified files to his home computer. The files detailed how the NSA both protects against cyberattacks and infiltrates the networks of others. Russian hackers were identified as locating these files through popular antivirus software the contractor used.

The software was manufactured by Kaspersky Lab, a Moscow-based company whose antivirus software was used by the U.S. government until legislation was passed banning its use due to national security concerns. The company repeatedly denied its involvement in cyber-espionage or that it was in any way tied to or influenced by any government. These efforts escalated and Russian hackers began attacking networks of smaller commercial companies that were deemed weaker and more vulnerable. They were practicing, so to speak, to prepare for the real aim: our energy systems, including the electricity grid.

Fast-forward to the latest development, in which Russian hackers had infiltrated U.S. systems, including energy, nuclear, water utilities, and other sectors. The attackers had acquired the ability to shut off electricity, they just had not acted on it yet. Perhaps Russians rightly realize that Americans won’t stand for having their lights turned off by a foreign adversary. Tinkering with our elections may be tolerable for some, but most won’t tolerate having their lives jeopardized with energy disruptions.

It isn’t only energy networks that need to be on high alert against cybersecurity – most critical infrastructure is managed online. So what are we to do? One answer comes through distributed generation. Some cities have been working on microgrids that improve local grid resiliency. Our military is developing solar-based microgrids to ensure energy security and continued operation during emergencies and prolonged outages.

Solar, in particular, is more cost-effective than the diesel-powered generators commonly used during power outages. Solar energy also reduces the need to rely upon the supply chain for fuel delivery. These emergency preparedness efforts are a no-brainer for critical facilities like military, hospitals, and all levels of government. And, if states would allow for third-party investment and leasing in distributed generation, the number of partnerships and benefits quickly multiply.

Cybersecurity is a rapidly developing area of the law and our state is fortunate to have the Judge Alfred P. Murrah Center for Homeland Security Law and Policy at Oklahoma City University’s School of Law, right here in Oklahoma City. The Murrah Center is preparing the vital group of future lawyers with its focus on domestic terrorism prevention, domestic security insight, legal analysis, and counterterrorism.

The center’s annual event, the National Summit on Homeland Security Law, takes place April 19 at OCU Law and provides a unique opportunity that brings together experts in the field and provides information that is applicable to most everyone. Tickets to the summit are available to the public; more info is forthcoming and can be found on the school’s website, assuming your computer still has access to electricity, at law.okcu.edu.

Jim Roth, a former Oklahoma corporation commissioner, is an attorney with Phillips Murrah P.C. in Oklahoma City, where his practice focuses on clean, green energy for Oklahoma.