

# Energy Diplomacy: USAID and USEA Enhancing Cybersecurity in Eastern Europe



By William Polen, Senior Director, United States Energy Association,  
and Annabelle Lee, Nevermore Security



energy security in Eastern Europe – the ability to provide access to affordable and reliable sources of primary and secondary energy to the population – is a function of natural resource endowment, the ability of markets to generate capital investment required to build out energy infrastructure, the geopolitics of natural gas and electric power transmission, and the security of power and gas grids.

For the fragile young democracies of the region (Armenia, Albania, Bosnia-Herzegovina, Georgia, Kosovo, Moldova, Montenegro, North Macedonia, Serbia, and Ukraine) a secure and diversified supply of energy resources is essential to support long term economic growth and social cohesion.

Since the fall of the Soviet Union, the United States Energy Association (USEA), in cooperation with the United States Agency for International Development (USAID), has worked in Eastern Europe to enhance energy security through the Energy Technology and Governance (ETAG) Program.

This is the second of a series of articles that describes the ETAG Program, its work in the region, and its tangible benefits to the United States.

### Cybersecurity is Energy Security

Though power grids in Eastern Europe are less automated than their Western European counterparts, the potential disruption to electricity service resulting from a cyberattack on critical infrastructure is a significant and immediate challenge to national and regional energy security.

In 2015, a first of its kind cyberattack committed against a Ukrainian distribution company resulted in two hundred and twenty-five thousand customers losing power for several hours. It took Ukrainian officials several hours to restore service.

The most debilitating effect of this and similar attacks on Eastern European critical infrastructure is the loss of confidence in government’s ability to protect its citizens and their fragile young democracies from the malign influence of state and non-state actors working to destabilize the region.

Scott Aaronson, vice president of security and preparedness at the Edison Electric Institute emphasized the significance of critical network infrastructure at the 2019 NARUC Winter Policy Summit, stating, “An attack on critical infrastructure is an attack on civil society.”

In response to the growing threat to energy security posed by cyberattacks on critical infrastructure in Eastern Europe, USAID and USEA launched the Utility Cyber Security Initiative (UCSI) soon after the attack on Ukraine.

### Re-Inventing Corporate Governance

Eastern European transmission and distribution utilities are unprepared for the challenges associated with cyberattacks.

Senior management does not have a comprehensive view of

### USAID and USEA organized an Energy Utilities Cyber Security Summit in cooperation with EEI to increase cybersecurity awareness of UCSI utility CEOs.

the magnitude of the threat and risk to business continuity; management has inculcated a minimal culture of cyber hygiene; boundaries between information technology and operations technology limit intra-utility coordination across potential attack planes; lines of authority for cybersecurity are not clearly delineated across management domains; budgets are siloed and this adversely impacts cybersecurity investments, as they are cross-cutting; most utilities possess only a basic cybersecurity awareness program focused on all employees; and supply chain management is rarely considered.

As a result, Eastern European utilities need to develop the management hierarchy, processes and procedures to effectively identify and implement cybersecurity controls and plan for, and respond to, cyberattacks. And, they lack an overall cybersecurity strategy that is necessary to advocate for cybersecurity investments in tariff discussions with their national regulatory authorities.

In the early 1990s, USAID and USEA pioneered the Utility Partnership Program, through which volunteers from American investor-owned utilities mentored their Eastern European counterparts during their transition from state owned entities to commercial companies. Today, the UCSI is working with the

**William L. Polen** is the Senior Director at the United States Energy Association where he directs the multi-year Energy Technology and Governance Program in cooperation with the United States Agency for International Development.

**Annabelle Lee** is the President of Nevermore Security where she

focuses on cybersecurity strategy and risk management; design and architecture; assessments against standards and applied cryptography.

The opinions expressed herein are those of the authors and do not necessarily reflect the views of the U.S. Agency for International Development.

same Eastern European utilities to re-invent their corporate management in the age of cybersecurity.

The UCSI is assisting utilities to develop a rational approach to cybersecurity capital expenditures by advancing a risk-based assessment methodology customized to the technology and business practices of Eastern Europe. The methodology enables utilities to identify and prioritize their most acute cybersecurity challenges based on the potential risk to reliability and business continuity. Utilities will use the methodology's results to justify near term cybersecurity capital expenditures in tariff discussions with their national regulatory authorities.

To foster longer-term cybersecurity planning, UCSI is conducting Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) assessments with its member utilities. The ES-C2M2 enables utilities to evaluate, prioritize, and set goals for improving cybersecurity capabilities in several management domains, including, but not limited to: risk management; asset, change, and configuration management; identity and access management; threat and vulnerability management; situational awareness; event and incident response; and workforce management.

The assessments are helping the UCSI utilities and their regulators determine their current cybersecurity posture, set goals, target medium to long-term cybersecurity investment, and identify policies, procedures and training programs needed to fortify defense and response capabilities.

### Information Access

Accessing threat information, security updates, and information on new software applications is a challenge to Eastern European utilities on the periphery of cybersecurity information networks.

USAID and USEA organized an Energy Utilities Cyber Security Summit in cooperation with EEI to increase cybersecurity awareness of UCSI utility CEOs. Participants included executives from Avangrid, Berkshire Hathaway, Eversource, Exelon, Enel, North American Electric Reliability Corporation, and Southern Company.

Key points emerging from the summit: Cybersecurity is a leadership issue, not just an information technology issue. Inculcating a culture of cybersecurity must be one of management's top priorities. Senior leadership needs to be aware of the threats and vulnerabilities and set priorities, allocate resources, and create accountability. To be effective, cybersecurity must be included in all facets of the organization: human resources, supply chain, network planning, substation automation, and corporate structure.

People are a utility's greatest asset and weakest link. First and foremost, cybersecurity requires an aware and alert culture, particularly in addressing phishing attacks, which account for eighty to ninety-five percent of unauthorized access to systems.

Anti-phishing training and awareness is critical for all employees, not only those focused on cybersecurity.

Technology is not a silver bullet. Technology deployment absent competent people, support processes and an overall plan will not lead to cybersecurity.

Changes in technology results in new attack vectors. New grid technologies are introducing millions of novel intelligent components to the electric grid that communicate in more advanced ways than in the past. With alternative energy sources such as solar power and wind, there is increased connectivity across organizations and systems. Increased interconnections and new technologies result in a larger attack surface that may be exploited by potential adversaries.

Developing a circle of trust for information sharing is essential. Protection of critical infrastructure is a shared responsibility.

## Unprotected Eastern European utilities provide a potential laboratory and staging ground for malicious actors to perpetrate attacks against American critical infrastructure.

Coordination among industry and government stakeholders and with other sectors, including water, transportation, and communications, will improve situational awareness, resilience, and security of the grid by sharing best practices, threats, vulnerabilities, cyber incident reports and mitigation strategies.


### Protecting Homeland, Extending Influence

Small American utilities share many of the same cybersecurity challenges as their colleagues in Eastern Europe.

Participating in USAID/USEA cybersecurity workshops and seminars provide American utilities volunteers with an opportunity to exchange knowledge and experience with their Eastern European counterparts.

And, as unprotected and unprepared Eastern European utilities provide a potential laboratory and staging ground for malicious state and non-state actors to perpetrate attacks against American critical infrastructure, improving the cybersecurity capabilities of Eastern European utilities protects U.S. utilities.

Volunteers in the USAID/USEA program provide invaluable contributions of time, expertise, and insights. USAID/USEA funds the cost of travel, lodging, insurance, meals, and other expenses associated with participation in the USAID/USEA cybersecurity program.

If improving energy security in Eastern Europe appeals to your firm, please contact us about opportunities to participate in the USAID/USEA Utility Cybersecurity Initiative. 

## Strategizing and Implementing

(Cont. from p. 59)

technical information with your peers or, perhaps, even the federal government that is specific about your network or your systems so there's a balance on how much information you share. There's also a concern about I may share information, but I'm not getting the same value in return.

Some of my larger utility clients who have sophisticated threat intelligence and security monitoring were providing a lot of information into the information sharing organizations. It's the right thing to do, but they weren't always getting a return from others because they were more sophisticated.

Then, you do have a similar concern with the government. The government would like you to share as much as you can but, because of security clearances and perhaps ongoing investigations or other matters, there's only so much that can be shared back with you.

**PUF:** What about the whole supply chain? You would be one of the first to see that and to say, how do we address that?

**Brad Bauch:** We do, and across the sector, there's a lot of work being done in the supply chain area and, more broadly, of the third-party risk management space because we're concerned about information and access that service providers may have, contractors may have, or the vendor that provides supports for your relays in your substation may have, for example.

Do they have physical access to your substation, or do they have remote access if they need to do firmware upgrades? That is a significant concern in the industry, in addition to security of the products themselves. Where are we sourcing the products, where do the firmware updates come from, where was the source code developed?

There are some emerging standards around supply chain security. You're probably familiar with the NIST security framework, as well as the NIST 800 security controls. There are specific controls around supply chain security, and there are new NERC CIP standards to address supply chain security.

**PUF:** Utilities generally need to have their investments and costs approved by utility regulators. Maybe they don't have a good understanding of what are the needs, and should they be spending more or less. Isn't that difficult?

**Brad Bauch:** It's always a challenge, the ratemaking process, justifying the spend. The best approach is to take a risk-based approach, so you need to understand the risks of the business, quantify that risk, and use a risk-based approach to manage that risk from a cybersecurity perspective.

You can't do cybersecurity just for the sake of cybersecurity, and you can't continue to use what we traditionally called FUD, fear, uncertainty, and doubt to justify your cybersecurity spend. You need to take a risk-based approach and then tie the projects and the spending to the risk reduction. Then you can show a risk-based return on that investment.

**PUF:** How do you think about the future and how to work that?

**Brad Bauch:** One of the most important things, and not to just keep beating that topic, is to continue to think about it from a risk-based perspective, understanding the threats, understanding the risks of the business, and focusing your spend and your efforts on what's important. The other is using more analytics and perhaps even automation to improve your visibility and your detection capabilities.

We have so much information about our systems and what people are doing that we could start to do more analytics and understand what does normal look like on a system and, instead of monitoring for everything, just monitor and look for the anomalies.

**You need to take a risk-based approach and then tie the projects and the spending to the risk reduction. Then you can show a risk-based return on that investment.**

I don't want to say that it's simple, but I'll use the term straightforward, in some of the control systems and the real-time systems. If you think about a distribution management system or SCADA system, those are very purpose-built systems.

They do one or two things, and they do them well so, from a technology perspective, those networks should be easy to baseline. Here's what normal looks like, and then you monitor those systems for anything that is now abnormal or, even more proactively, you just block it. You only allow the normal baseline traffic to occur and you block everything else. Then you start to limit the attacks that could come in and the impact of those attacks.

The other thing that is important to continue to do is making sure that the boards are informed and knowledgeable on the cybersecurity topics. We're doing a lot of that now, and we're seeing boards becoming even more sophisticated from a cybersecurity perspective. Security leaders have to continue to increase their business acumen and not talk to the boards and business about technical things but talk to them about business risks. **PUF**

How did Bill Nye become "the Science Guy?" A comedian called him that when Nye correctly pronounced "gigawatt."