Testimony of

Timothy M. Yardley

Senior Associate Director of Technology and Workforce Development, Information Trust Institute, University of Illinois at Urbana-Champaign

Before the United States Senate Committee on Energy and Natural Resources

October 11, 2018

Introduction

Good morning Chairwoman Murkowski, Ranking Member Cantwell, and distinguished Members of the Committee. Thank you for the opportunity to speak today.

I am a Senior Researcher and Associate Director at the Information Trust Institute, University of Illinois Urbana-Champaign. My research focuses on cyber resiliency in critical infrastructure with a particular focus on the electric power grid. I also have a deep prior background in telecommunications and cyber security in a broad number of disciplines. I have worked on cyber resiliency research for critical infrastructure for over 10 years with funding from DOE, DHS, DARPA, and Industry. Much of the electricity subsector knows me based on the extensive testbed capabilities that I have built up at the University of Illinois and that have been a building block of many scientific advances made in this domain.

I have proposed and participated in a variety of research projects that have materialized into technology that is deployed on our electric grid today. I have been funded to work on areas covering the gamut of identification, protection, detection, response, and recovery. I have also been active both in assisting in the education of new minds through student interactions and in adapting existing workforce to the evolving modernization of a cyber resilient grid. Lastly, some of my current work focuses on providing portable testbed environments that allow for the verification, validation, and improvement of mission-critical cyber response tools aimed to aid in black-starting the electric grid amidst a cyber-attack. In short, my experiences provide me with a unique perspective to offer the Committee insight and recommendations concerning the cyber recovery of our grid when faced with a full or partial black start scenario.

In my remarks today, I will:

- Describe a broad viewpoint on cyber-preparedness for restoring the electric grid,
- Describe a need for research, development, and continuous engagement of both preventative and restoration toolsets,
- Describe the unique contribution universities (including the University of Illinois) play in developing new, innovative technologies and approaches to preventing, detecting, and recovering from cybersecurity threats to the grid,

- Emphasize the need to increase investment and innovate in approach for workforce development cyber-preparedness,

- Emphasize the need for more robust rehearsal of policy, skills, tools, and knowledge acquisition to carry out our global goals

Background

It is not news to anyone in this room that the critical infrastructure that is relied on throughout the world is under threat. In the news are many reports of information gathering and potential attacks against this infrastructure, including the electric grid. Cyber security researchers are uncovering campaigns, toolsets, and even some attacks that are targeting electric grids and the systems that operate them. It is also well understood that a compromise of the power grid control system or other portions of the grid's cyber infrastructure can have serious consequences, ranging from a simple disruption of service with no physical damage to potential permanent damage that can have long-lasting effects on the ability of the system to operate.

I rest assured that our nation is relatively prepared from a physical perspective to address the logistics of a traditional outage or black start scenario. I fear though, that we are still not prepared to do so in the face of a cyber-attack that eliminates our ability to trust the systems we use to operate our grid. There is urgency necessary in closing that gap.

Cyber Security Funding

For over a decade now, much attention and funding has been placed on cyber security for the grid, but cyber resiliency is much more than just cyber security and is only recently gaining focus. That money has been well spent and there is a continued need to fund the protection of our electric grid from adversarial manipulation. However, as has been shown repeatedly in the media, a determined adversary will eventually succeed, so what do we do then? While the attacks of the past were often focused on the business side, it is becoming more concerning that the toolsets are migrating to operational technology (OT) specific functionality. Are we prepared? Unlike the examples so far in the media, the U.S. grid is arguably more resilient to failure but just because it is harder to topple, doesn't mean that it isn't possible. Cyber Resiliency as an approach, is a potential answer.

Given that protection cannot be made perfect, and the risk is growing, cyber resiliency is critically important. Cyber resiliency aims to protect through established cybersecurity techniques, but acknowledges that such protections can never be perfect, and requires monitoring, detection, and response to provide continuous delivery of electrical service. While some solutions from classical cybersecurity can support cyber resiliency (e.g., intrusion detection and response), the majority of the cybersecurity work to date has focused on preventing the occurrence of successful attacks, rather than detecting and responding to partially (or fully) successful attacks that occur.

One of my most relevant research efforts falls under the DARPA Rapid Attack Detection, Isolation, and Characterization Systems (RADICS)[1] program lead by Mr. Walter Weiss. The goal of that program is to enable black start recovery of the power grid amidst a cyber-attack on the U.S. energy sector's critical

[1] https://www.darpa.mil/program/rapid-attack-detection-isolation-and-characterization-systems

infrastructure. RADICS research is developing technology that cybersecurity personnel, power engineers, and first responders can utilize to accelerate restoration of cyber-impacted electrical systems. One of the key tenets in this program, and part of my role, is the development of testbed environments and aiding in the creation of an exercise format that enables the evaluation and improvement of these technologies as they are developed. By creating these environments and developing scenarios that allow practitioners to put these tools to work, great progress can be made on preparedness as we invest in cyber resiliency.

In current viewpoints, many look at testbed environments as a piece of a bigger puzzle, but not as an area of focus on its own. That needs to change and the full potential of testbeds and their capabilities need to be realized. Imagine a facility that allows you to test your theories and new techniques on systems that truly operate like the real world, but without the capital and time expenditures necessary to deploy those on the real system. Imagine a facility that allows next-generation products to be configured, tested, and validated iteratively during development to build a more robust product and a stronger overall solution. Imagine that same facility being used to train your current and future workforce on the systems they use in the real world, with behaviors that match, with their own configurations, and do so in matters of days or weeks rather than months or years. Imagine that same facility being used to continuously train our first responders so that they are prepared when they are called upon. Now, use that facility to look at these scenarios in face of adversarial manipulation and TTPs. Such a facility doesn't fully exist today, but great strides have been made to realize aspects of that at the University of Illinois as well as at DOE National Laboratories. Much more work still needs to be done and with the right combination of teams, it can be realized.

Testimony has been previously given to this committee on the importance of cyber resiliency, so I will not repeat that here. I do echo the importance and necessity of that path. Testbeds are a cornerstone of understanding how we are improving on cyber resiliency as we progress down that path. Instead of focusing on resiliency though, I will focus on some specific aspects that may help as we continue to harden our systems that protect critical infrastructure.

Focus on Exercising Essential Items

With FAST Act authority, there are new powers for taking action when action needs to be taken. There remains a question as to what those actions may be and when they are appropriate to take. Recent work by Paul Stockton[2] and others have identified needs to look at templates and think through the scenarios that make sense for leveraging these powers and putting the right protections in place. This is a critical piece that will take time and effort to work through, with a variety of stakeholders at the table. This is time that must be spent.

Cyber security workforce education is another area that takes time to work through. There is a saying that we are only as strong as our weakest link, and when put into context of cyber security that weakest link is likely our staffing. Many organizations will have cyber security focused staff on hand as well as third-party entities that are contracted for response actions. Are there enough of them? Are they truly prepared to respond to a critical infrastructure attack at scale? What about the national guard and others that can be called upon? How do we make sure all of these people have the tools, skills, knowledge, and pre-existing relationships so that if an emergency black start cyber-involved scenario

[2] http://www.jhuapl.edu/Content/documents/ResilienceforGridSecurityEmergencies.pdf

ever occurs, they are ready to hit the ground running? How do we guarantee that their skills are fresh and not "rusty" from lack of use? This is a difficult problem that traditional training can't fully prepare one for, so we have to think outside the box and we have to evolve how we train people. Testbeds are a partial solution, but more focus is needed to advance that further and it still needs a pipeline of people. Staffing in a large-scale emergency response is often one of the most difficult undertakings, so we need to address it pro-actively and increase the breadth of resources now.

What do you train the people on though? The base systems will need training, of course. The traditional cyber security and forensic response tools as well. What about those tools that are built for cyber-physical environments like the electric power grid? Further focus needs to be spent on assembling what that toolkit looks like and to fill the gaps on what is missing. Some work is being done in this space, but more focus needs to be placed on it.

Academic Involvement (NSF/DOE/DHS/DARPA)

Many of these cyber-resilience findings being discussed today have grown out of collaborative academic-industry-government settings, including several major research activities that I have led or participated heavily in. Funding for these efforts has been broad, indicating both the importance and the complexity of these problems. In my time in this area, I have been involved in funding from Industry, NSF, DOE, DHS, and DARPA all taking on a particular piece of this problem space. Some of those efforts include the Trustworthy Cyber Infrastructure for the Power Grid projects (TCIP, 2005–2010; and TCIPG, 2009–2015), the Critical Infrastructure Resilience Institute (CIRI, 2016-2020), the Cyber Resilient Energy Delivery Consortium (CREDC, 2016-2020), and the Cyber Physical Experimentation Environment for RADICS (CEER, 2016-2020).

It is my belief that we must not just innovate but that we must put into practice the knowledge that comes and the tools that are created. Once knowledge is disseminated and tools are created, they must continue to use these tools regularly so that the tools can continue to improve and advance rather than be behind the glass and not touched until they are needed. All of these are partnerships between academic institutions, national labs, government sponsors and stakeholders, and most importantly with Industry. Across these efforts, the team of collaborators have worked together to understand, improve, and enable critical work across the target critical infrastructure domains. In both technology and impact, each of these have had their own successes including creating multiple startup companies and transitioning multiple technologies to industry (including Grid Protection Alliance, First Energy, Schweitzer Engineering Laboratories, ABB, Honeywell, Ameren, Telecordia, GE, Entergy, EPRI, DTE Energy, and PJM, among others). The projects also have had a significant positive impact on workforce education, delivering successful short courses, producing graduates, conducting hands-on training, and providing the base knowledge necessary to do this type of work by others.

While progress is being made, further work is critically needed to define cyber resiliency architectures that protect against, detect, respond to, and recover from cyber-attacks that occur. Some specific guidance about cyber resiliency research that is critically needed comes from a consensus study published in July 2017 by the National Academies of Sciences, Engineering, and Medicine entitled "Enhancing the Resilience of the Nation's Electricity System."

Timothy M. Yardley, Senior Associate Director, Information Trust Institute, University of Illinois Urbana-Champaign

Summary

The cyber threat to grid resiliency and the reality of a potential black start scenario is real, and the time to act is now. It is critical that the committee understands the following:

1) A lot of existing work has been done, and that work is tremendously important. However, our effort needs to think broader and look at the problem from a cyber resiliency perspective rather than just cyber security.

2) We need to focus on increasing the capabilities of our people as much, if not more, than we focus on our technology.

3) We need to think through the policies, procedures, people, skills, tools, and the requirements necessary for those items to function before they are needed.

4) These capabilities can be achieved only if academia, industry, and government work closely together in a focused research, development, and education program.

5) Congress should continue to fund and increase funding to DOE and other government agencies to advance this research with broad engagement between Academia and Industry, building upon successes of the past.

Thank you for the opportunity to be here with you today. I would be happy to answer any questions that you have.