Georgia Tech Strategic Energy Institute Georgia Tech Institute for Information Security and Privacy

Preparing for the Inevitable: Cybersecurity Attacks and Our Energy Infrastructure

Prepared by Georgia Institute of Technology
Strategic Energy Institute
Institute for Information Security and Privacy

BACKGROUND MATERIALS:

Our country has a critical need to develop the advanced workforce and educational pipeline that is equipped to take proactive countermeasures to respond to the interrelated challenges of cybersecurity and critical energy infrastructure. The United States is increasingly vulnerable against the threat of cyberattacks that could impair our electric grid, network of oil and gas pipelines, and economy at large. To address this need, the federal government should fund a network of university-based centers to perform advanced R&D, develop a trained, globally competitive workforce, and the underpinning educational programs and resources to guarantee the U.S. workforce remains adaptable to emerging threats. These centers should be distributed regionally across the country in order to address each regions distinctive characteristics, and to partner with regional utilities, national labs, regulatory and policy bodies, and coordinate closely with relevant federal agencies, such as DOE and DHS. These regional centers can elevate the quality and quantity of human capital resources that understand the convergent challenges of clean, reliable electric power and cybersecurity under a nationally-coordinated program.

BACKGROUND:

The possibility of weaponizing energy infrastructure and control systems through cyberattacks by rogue entities is a growing concern. The positive trends of digitalization, decentralization, and decarbonization are transforming the US electric energy system which creates new challenges in protection, control and operation of the system. With these news trends, also comes the development of a geographically dispersed cyber infrastructure and approaches to confront previously unknown technical problems. The operational reliability and security (resilience, self-healing, intelligent and autonomous controls) of the electric energy systems is tightly coupled to the cyber security of its infrastructure. Because of these complex systems, our country must have the trained workforce to address these challenges across a broad spectrum of emerging needs. They must also be able to draw regionally from a competent well-prepared talent pool that has been educated by leading institutions. Companies in the utility and industrial sectors find it very challenging to recruit high quality talent with concurrent expertise in cybersecurity, critical infrastructure and the physical and regional domains of interest. Attention and funding is needed to secure the trained workforce for the critical energy infrastructure and networks, including the electric grid, and oil and gas pipelines[1]. Employment of information security analysts is projected to grow 32 percent from 2018 to 2028[2]. However, recent research shows 1.8 million more cybersecurity professionals will be needed to accommodate the predicted global shortfall by 2022[3]. Workers in their department, and a majority believes that it is a result of a lack of qualified personnel[1].

In addition, the electric energy systems are coupled with other critical systems, such as oil and gas pipelines and, increasingly, transportation networks, including electrified transportation. The security of networked critical infrastructure has never been more critical. This is particularly true for the U.S. electric grid due to the evolving generation mix and increase in the probability and severity of threats-whether private, state or terrorist-funded. While our new sources of energy have many positives, they also have the potential to increase vulnerability and the number of access points. Current cybersecurity tools, technologies and countermeasures have been largely developed around a centralized electric power grid, however, significant shifts in our energy resources, including renewable wind and solar, grid-scale battery storage, producer/consumer ("prosumer" models), transactive controls, and device-level sensors, are proliferating more quickly than threat detection and reduction systems can keep pace. Moreover, the range of new players in this increasingly distributed system will introduce new challenges in balancing personal privacy, data privacy, and security. Furthermore, regional differences in infrastructure, energy resources, network communication systems, and demand-side considerations for residential, commercial and industrial loads, will necessitate that future cybersecurity protections be customized to the needs of each region.

"The fact is we need to educate and train individuals in cybersecurity at all levels, and it requires not just degrees but different types of certifications as well as continuing education for those already in the workforce." [4]

CURRENT RELATED CENTERS/THRUSTS:

Currently, a number of electricity-cybersecurity initiatives are being led by the DOE lab complex. This is a good start but does not sufficiently address all aspects of this challenge, particularly workforce development needs. Good models exist today, such as the CREDC center at University of Illinois Urbana Champaign, as well as smaller scale efforts led by teams of individual researchers through DOE grid-modernization initiatives. These approaches represent models that must be significantly expanded. A broader network of university based, regional cybersecurity centers are needed to tap into the knowledge base of regional stakeholders. Such centers would directly align with and complement the mission of DOE and its relevant cybersecurity and electric grid activities. These should be defined by specific regional needs and distinctive strengths yet pay into an increasingly well-trained pool of workers across the country. These centers will also develop the local workforce with a range of educational backgrounds that understands the dual challenges of clean, reliable electric power and cybersecurity.

RESPONSIBILITIES/THRUSTS OF THE REGIONAL CENTERS:

These regional centers should have the following specific responsibilities and thrusts. While some of these aspects are already being performed, there is a need for holistic, concentrated efforts that are regionally distributed:

- Workforce development for energy system operation, security, and cyber security
- Development of an educational pipeline of skilled undergraduate and post-graduate talent
- Cybersecurity research
- Operational security of electric energy systems research
- Operational security of other interconnected/interdependent infrastructure research

- Cyber-physical laboratory development for hands-on training of next generation engineers
- Industry engagement and professional training
- Research and capability development to monitor cyber activity and threats to the electric energy system
- Strengthened university and/or affiliated UARC partnerships with national labs for fast response team to cyber physical attacks
- Cybersecurity management and policy
- Development of training materials specific for critical infrastructure cybersecurity

MODELS FOR THE REGIONAL CENTERS:

The centers would be R&D focused, and by being based out of universities, would be necessarily training a cohort of students with a range of educational backgrounds. In addition to R&D, we would see the centers as being responsible for course development, training, workforce development, and regional outreach. These centers will have a suggested scale on the order of $5M/year for 5 years. These would be distributed around the country, targeting a number of around five (given that the US has 3 interconnects and 8 NERC regions).

These centers would have a governance structure with strong public-private oversight of the center activities, including EPRI, EEI, National Labs, PSC's, utilities, OEM's, etc. The R&D would necessarily leverage the distinctive capabilities of universities at earlier stage research, but would also prioritize problems/challenges associated with their regional distinctives - the public/private steering group mentioned above would both bridge the gap/accelerate the earlier stage work and application, but also to point the fundamental research in the direction of "use-inspired" research problems of the region. Finally, workforce development/job creation would be a key aspect, with particular attention to equitably addressing the disparate challenges and vulnerabilities faced by both urban and rural areas.

CONTRIBUTORS:

Sakis Meliopoulos
Santiago Grijalva
Raheem Beyah
Angels Keromytis
Alexa Harter
Wenke Lee
George White
Rich Simmons
Sharon Murphy
Tim Lieuwen

REFERENCES:

1. Frost - 2017 - 2017 Global Information Security Workforce Study.pdf.
2. Santos, D., Goel, S., Costanzo, J., Sagen, D. & Buddelmeyer, P. A roadmap for successful regional alliances and multistakeholder partnerships to build the cybersecurity workforce. NIST IR 8287 https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8287.pdf (2020) doi:10.6028/NIST.IR.8287.
3. Chairwoman Johnson Opening Statement for Cybersecurity Workforce Hearing | House Committee on Science, Space and Technology. https://science.house.gov/news/press-releases/chairwoman-johnson-opening-statement-for-cybersecurity-workforce-hearing.
4. Information Security Analysts : Occupational Outlook Handbook: : U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm.