TCIPG

Smart Grid Cyber Security: Training for the Future

Tim Yardley

GOALS

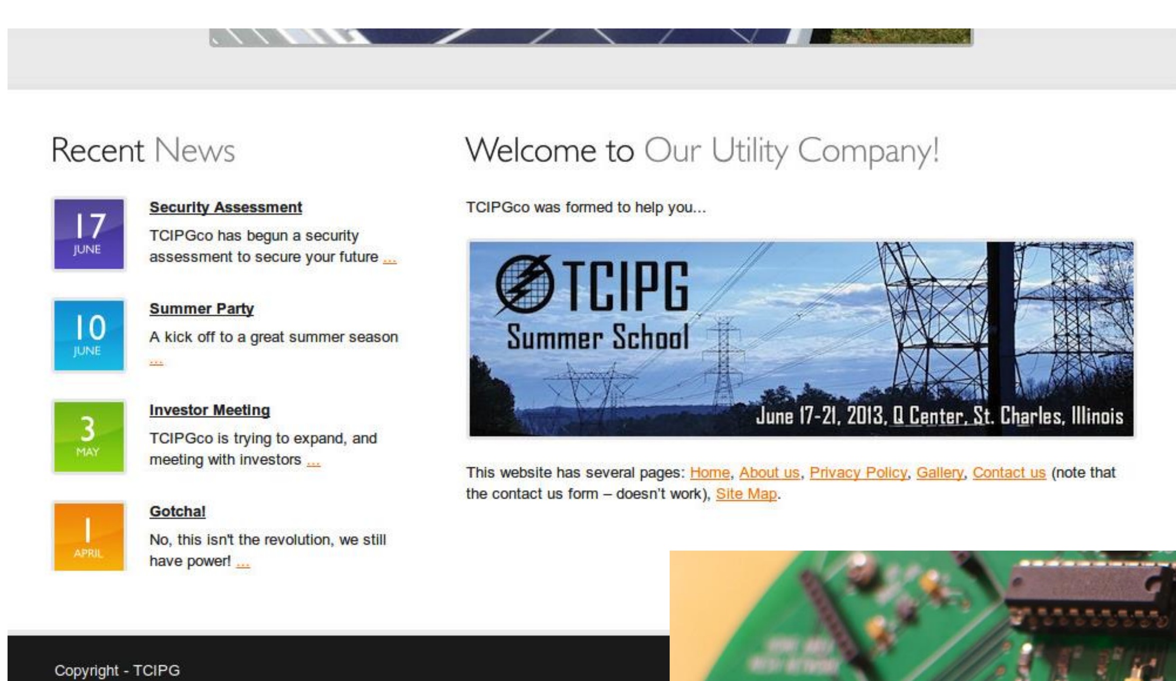
- Develop an open, modular, phased learning platform for cyber security education in the electric power grid.
  - Covers diverse topic areas spiraling deeper into relevant details of interest (tracks).
  - Consists of lecture material, an electronic exercise environment, and hands-on exercises to support learning.
- Provide a fully open, available, and vetted curriculum.
  - Material needs to be widely usable; different experts should be able to easily contribute new content and revise existing content as the landscape changes.
  - Made to be accessible to anyone (ranging from CEOs to engineers to office staff) while taking a project-based, hands-on, active-learning approach to reinforce the subject matter.

FUNDAMENTAL QUESTIONS/CHALLENGES

- What gaps exist in the current training?
- How do existing training options map to job responsibilities and competency needs of the sector?
- What can be done to bridge the gaps that exist and to train for the future of the smart grid?
- How does one create a self-standing curriculum that can educate a broad audience on an advanced and emerging topic?
- What areas of information are truly useful for professionals in this field?

RESEARCH PLAN

- This effort started with an initial gap analysis and mapping of existing cyber security training for the electric power grid, in relation to the DOE Secure Power System Professional (SPSP) and DHS National Initiative for Cybersecurity Education (NICE) competencies and job responsibility designations.
- Gather topics of interest and sector needs by working with industry and leveraging existing knowledge of the sector.
- Based on the gap analysis, a core curriculum is being developed that includes a combination of new material and material from previous TCIPG short courses on cyber security in the electric power grid. It is structured to facilitate easy extension into new areas.
- The material follows a phased approach to learning that includes active, project-based "learning by doing" to anchor the training material.
- Prepare lectures with hands-on exercises to reinforce the material under discussion.
- Release the training in stages, and revise it for future use in response to feedback from participants.
- Ongoing analysis will be conducted to determine coverage and needed topics for future releases.



RESEARCH RESULTS

- Gap analysis has been conducted, along with a mapping to job responsibilities and competencies.
- Preliminary curriculum has been created.
  - Several modules have been alpha-tested in the field with industry participants.
- Topical spirals into more detail are being developed.

TOPICS COVERED

- Power fundamentals
- Cyber security fundamentals
- Communications and networking
- Cyber infrastructure in the electric power grid
- Monitoring and situational awareness
- Advanced metering infrastructure
- Smart grid guidance documents
- Electric sector capability maturity model
- Privacy in the smart grid
- Critical infrastructure security examples and impact
- A perspective on security
- Security challenges in distribution automation
- Embedded assessment
- SCADA fundamentals
- Robust control systems
- And more…

BROADER IMPACT

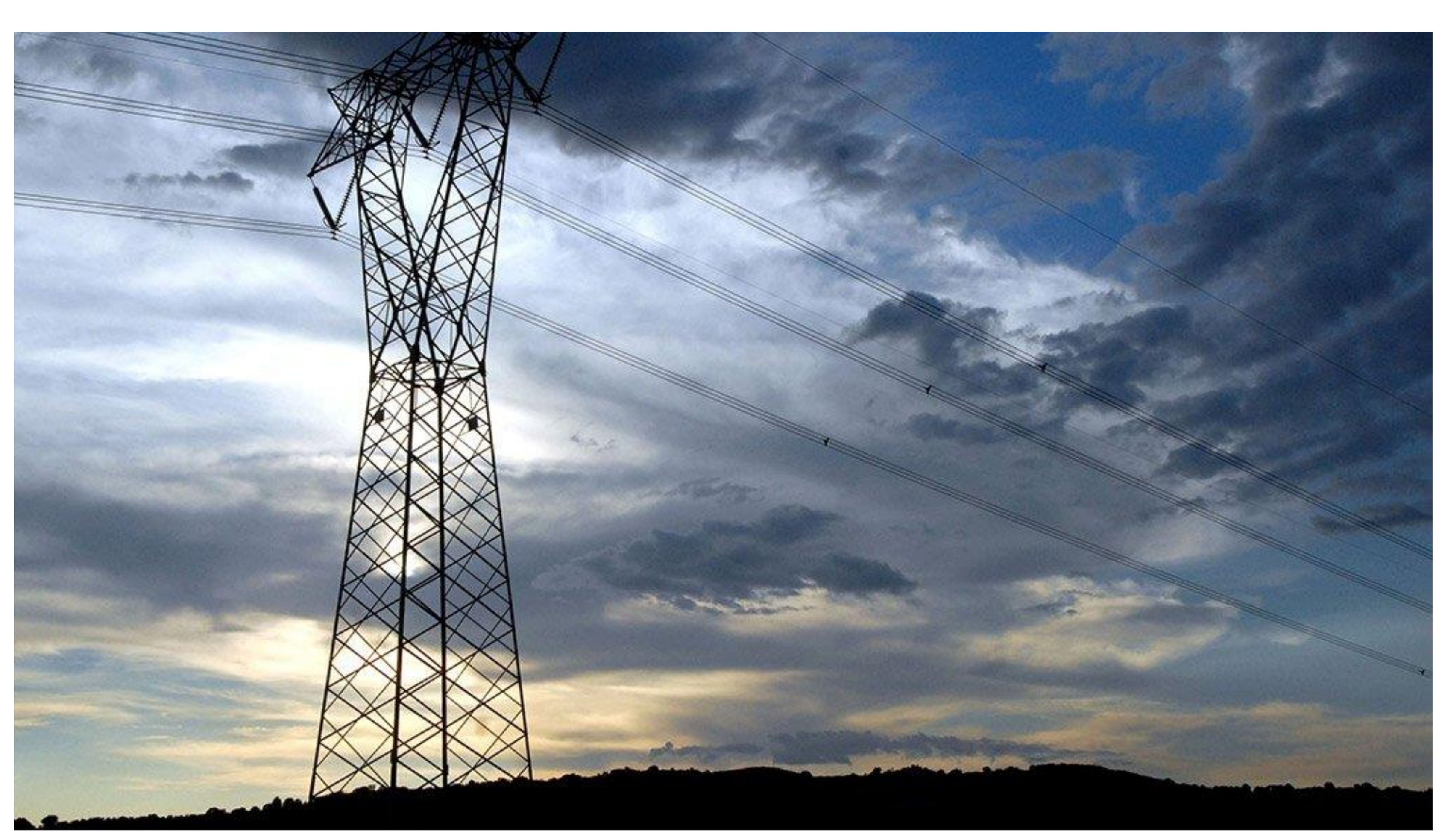
- The training reflects the broad expertise of the TCIPG research team and acts as a training platform that future researchers, workforce, or government entities can build upon and adapt.
- Offers open, widely available training material on cyber security in the electric power grid that has been vetted by subject matter experts.
- Increased access to training in the domain.

FIELD USE

- Prior incarnations of the lecture material and short courses have been used to train hundreds of attendees from academia, industry, and government.
- A very early version of the revised lecture material was used at the 3CS conference to provide training for community college educators and other interested parties.
- Modules of the core curriculum have been used to train vendors and utility personnel in this domain.
- Strong continued industry interest in the material.

FUTURE EFFORTS

- Full open-source release planned for August 2015.
- Explore integration and use with other efforts, such as cybatiWorks or the SANS curriculum.



TRUSTWORTHY CYBER INFRASTRUCTURE FOR THE POWER GRID | TCIPG.ORG

UNIVERSITY OF ILLINOIS | DARTMOUTH COLLEGE | UC DAVIS | WASHINGTON STATE UNIVERSITY

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T