Cyber security challenges for the power grid from R&D and policy perspective

Manimaran Govindarasu, Iowa State University

Modern power grid is a complex cyber-physical system that increasingly relies on smart sensors, real-time communication networks, and distributed controllers for efficient monitoring, protection, and control of the grid. While these cyber components have contributed to increasing efficiency, reliability, and economic operation of the grid, they also have resulted in increasing grid's cyber attack surface. In recent years, cyber threats and attacks have increased both in numbers and sophistication, and also evolve rapidly. The legacy nature of the grid coupled with slow adoption of new technologies within exacerbates this problem further. In this context, the following are some of the R&D and policy suggestions. In the panel, only a subset of these suggestions (2 or 3) will be discussed.

- Develop a **holistic cybersecurity framework** that encompasses attack deterrence, prevention, detection, mitigation, resiliency, and forensics.

- Develop **pragmatic risk assessment models and risk mitigation strategies** that account for adversarial behaviors, cyber vulnerabilities, and the system impacts. Develop techniques/tools to reduce attack surface.

- Enable paradigm shift from the traditional notion of **fault-resiliency to attack-resiliency** to address emerging man-made malicious events beyond the conventional faults that are often due to naturally occurring extreme events.

- **Accelerate innovation of Operational Technologies (OT)** so as to bridge the gap between IT and OT and to ensure seamless convergence of IT and OT in operational environments.

- **Continuously improve the compliance** requirements (e.g., NERC CIP) to the extent of verifying the effectiveness of process, technologies, and the people who operate/manage the system, and make the compliance process adaptable and sustainable to emerging needs.

- Extend NERC **CIP-like requirements to distribution grids** that are often lack adequate protection against cyber attacks.

- **Develop realistic testbed infrastructures**, with associated models and data sets, with the goal of bridging theory to practice, and accelerate innovation and deployment in this area. Incorporate testbed-based scenarios in NERC GridEx.

- **Facilitate synergistic partnership** among industry, universities, and federally funded laboratories to not only advance the R&D, but also to educate/train skilled workforce in a sustainable manner.