Thanks for allowing my participation in the grid security talks today. I found much of the material interesting and it was a good chance to link up with a number of colleagues, as well as visit the NAS for my first time … that was great!

Based on what I saw and heard today, and following a recommendation from Jeff Dagle, I have something to add to the public record. Thanks and here you go:

Comments

1. The name Michael J. Assante (RIP) was invoked several times today. As I counted him as close friend and mentor/colleague, I'd like to reprise one of the statements he made on multiple occasions: "While necessary, cyber hygiene, even if done at a high level, registers as barely a speed bump for certain classes of well-resourced cyber adversaries." With the exception of remarks made by Mr. Tim Roxey, everything I heard today was on the level of cyber hygiene… as in: necessary, but far from sufficient for thwarting top tier attackers.

2. Remarks made by Ms. Samara Moore, (who I also count as a friend and colleague), spoke of potential security gains that might be made should the electric sector move more of its appropriate functions and data to cloud services providers who, due to the nature of their business, are incented to perform and deliver cyber hygiene best practices at a very high and sustained level. For selected utility functions, I concur with Ms. Moore's contention that the cloud holds promise for improving security posture.

3. However, one of the mantra's of my colleagues at the Idaho National Lab is: "If you are critical infrastructure you will be targeted, and if you are targeted you will be compromised." While on first hearing this may sound extreme to some, in practice it is a demonstrable fact.

4. Mr. Roxey attempted to address our unfortunate current condition of having become so utterly dependent on highly complex automated systems that far outstrip our ability to understand, let alone defend, them. Far from hopeless, however, he posited that a selective re-introduction of grid elements that could be proven safe and secure by deterministic methods would go a long ways towards increasing our confidence that normal grid operations might be maintained, even in the face of targeted, nation-state-level cyber campaigns.

You may recall, towards the end of his allotted time, Mr. Roxey read aloud the following draft policy language he urged us to consider:

> *Those systems, structures, or components deemed necessary to protect the "health and safety" of the public (for nuclear) or deemed highly critical via appropriate regulations (for non-nuclear CIKR)* ***SHALL*** *be protected by systems that can be shown effective via* ***Deterministic Methods.***

You may also recall that not only was there little time for participants to explore the underlying meaning and ramifications of this sentence, there were also very few in attendance with the right skills sets or experience to do so. No offense intended, this is a highly esoteric domain.

Recommendation

As soon as is practical, I recommend the NAS convene a group of scientists and other subject matter experts to explore Mr. Roxey's concepts in much greater depth than was possible today. Expertise in grid physics, grid operations, OT cybersecurity and procurement will be required to help the committee make the most of time exploring this strategically urgent topic.

Links to Relevant Papers

- "Surviving on a Diet of Poisoned Fruit: Reducing the National Security Risks of America's Cyber Dependencies". Richard Danzig, CNAS, 2014.

  https://s3.amazonaws.com/files.cnas.org/documents/CNAS_PoisonedFruit_Danzig.pdf

- "The National Security Case for Simplicity in Energy Infrastructure". Michael Assante, Tim Roxey, Andy Bochman, CNAS, 2015.

  https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151030_Assante_SimplicityEnergyInfrastructure_Web.pdf