Contribution ID: **352**

Type: **Paper**

Prioritizing Actions for Managing Cyber Security Risks

Monday 10 February 2020 17:30 (15 minutes)

Cyber incidents are the norm in every industry, and the nuclear industry is no different. However, the effects of an incident are different in the nuclear sector, where consequences are heightened by fears of radiation releases and material diversion. In an era of fake news that often spreads on social networks quicker than accurate official reports, incident planning needs to be prioritized and given a fresh look.

That was just one finding from a workshop on nuclear cyber risks held in Vienna, Austria, in late 2018. The Fissile Materials Working Group (FMWG) - a coalition of 80 organizations from around the world working to keep the world safe from nuclear terrorism - in collaboration with the Stimson Center brought together cybersecurity experts and stakeholders to consider cyber risks in the civil nuclear industry and how to address them. The workshop report, Nuclear Cybersecurity: Risks and Remedies, details 10 findings.

Since the time of that report, FMWG and Stimson have been working with expert stakeholders to further assess those risks, to consider new emerging risks, and to prioritize actions needed to better manage them.

In the cyber incident management example, it was found that more scenario-driven exercises are needed, as well as joint development of possible approaches to misinformation and the creation of an "accurate news" repository. With artificial intelligence (AI) now assisting the development of "deepfakes,"disinformation has become an even greater challenge to officials looking to convey appropriate emergency information after a nuclear/radiological event. Efforts to develop good approaches to this challenge should be coordinated with IAEA emergency response work and could be exercised through both new and existing forums, such as the Global Initiative to Counter Nuclear Terrorism (GICNT) exercises.

The issue of secrecy in security also presents a sector challenge, with management of nuclear security being more close hold than in some other sectors. One way to address the requirement for secrecy is the establishment of an anonymized database comprising lessons learnt regarding security incidents, be they accidental/intentional or cyber/physical/combined. An "operator database"resource should be developed from opensource reporting and voluntary sharing and may include safety incidents with cyber-components. The database should also include incidents on industrial control systems from other industries that could affect the nuclear sector.

New approaches are needed to reduce risks. Some, for example, have suggested nontargeting of nuclear power plants including via cyber intrusions. But to enforce agreement on this, cyber attribution would be needed. This paper will detail some new work being done in the private sector and civil society to help with attribution.

The paper will also consider new technologies. Unmanned aerial vehicles and wearable digital devices already threaten information security and potentially nuclear facility operations. Some even newer technologies can also be a help to security as well as a threat. For example, robotics and remotely-operated weapon systems all can assist in making security more cost efficient and could be an effective attack deterrent. However, these also present additional attack surfaces for cyber intrusion. An understudied factor is any catastrophic incidents occurring from the misuses of new technologies and machine intelligence, which are so unknown, will almost certainly be unpreventable and beyond the design basis threat of any nuclear facility.

What is the nuclear industry to do? And what can governments do to help address these risks?

The original work of the first FMWG-Stimson workshop –an assessment of nuclear cyber risks and recommendations for addressing those risks –is in the process of being analyzed with input from dozens of expert stakeholders. This paper presents an updated analysis that considers even newer risks, recounts some of the work being done to address nuclear cyber risks and presents recommendations for actions to be undertaken to manage these risks.

State

United States

Gender

Female

Authors: Ms DECKER, Debra (Stimson Center); Ms RAUHUT, Kathryn (Stimson Center); Mr FABRO, Mark (Lofty Perch)

Presenters: Ms DECKER, Debra (Stimson Center); Ms RAUHUT, Kathryn (Stimson Center); Mr FABRO, Mark (Lofty Perch)

Session Classification: Risks and benefits to nuclear security from innovations in other fields, including artificial intelligence and big data

Track Classification: CC: Information and computer security considerations for nuclear security