Contribution ID: **133** Type: **Paper**

Methodologies and approaches useful for Cyber Threat Assessment and Cyber DBT along side with classical DBT methodology as stated in NSS-10 Document

Nuclear power plants and other nuclear facilities are considered among the most critical infrastructure assets vulnerable to cyber attacks leading to loss of lives, property destruction and economic upheaval. It is essential that these cyber threats be properly addressed considering their nature of risk at particular nuclear facilities. The classical methodology described in NSS 10 document for Physical threat assessment and physical DBT may not be sufficient to cover all the cyber threats due to a few differences in physical and cyber threats as described below.

The classical physical threat assessment process as described in NSS-10 document, starts with the identification of adversaries in the location of nuclear facility. Once you know the active adversaries, the investigating agencies and other stakeholders involved in the DBT assessment process, find out the characteristics of adversaries like Motivation, intension and capabilities. These characteristic data of adversaries is further analyzed in threat assessment and DBT process to get the most probable and realistic threat vectors against which the physical protection is designed and implemented to ensure the highest physical security for the nuclear facilities and nuclear power plants.

The differences in physical and cyber threats:

1. Cyber threats are a global phenomenon not only local.
2. It is not possible to know all the cyber adversaries, as they are spread all over the glob and not open or known in public as in physical adversaries.
3. No intelligent agencies can find out their characteristics like capabilities and intensions, as they are not open or known.
4. Cyber adversaries are location independent as they can attack from any where in the globe, which makes the task of intelligent agencies further difficult.
5. Cyber threats are more technology intensive than physical threats so as the technology advances, cyber threats are also becoming more advance. Cyber threats are more dynamic as compare to physical threats, which are more constant without much advancement in weapon technologies.
6. Cyber skill can be easily available and purchased or can be acquired in short time. So it is difficult for investigating agencies to clearly find out the capabilities of known cyber adversaries.
7. Cyber threats can be easily carried out without any deterrent (as in physical protection) as adversaries are always hidden. So cyber threats are more dangerous. It makes more essential to implement cyber threat assessment program more rigorously.
8. Cyber resources used in attack are easily available in the open market without any restriction and can be purchased without any issue and large funds as compare to physical resources.

Points 6,7 and 8 make the investigating agencies task more complex and difficult as with this adversary can develop the capabilities in very short time.

The NSS-10 document does not provide enough guidance to derived effective cyber security threat assessment and cyber DBT. The model of physical protection is not easily applicable to cyber defense. Moreover, describing the cyber threat landscape is not an easy undertaking, as has been discussed in several computer security consultancy meetings at the IAEA. The design-basis-threat approach (DBT) as described in NSS 10 is insufficient to cover cyber threat problem.
The Paper presentation will discuss the approach and methodology of cyber security threat assessment and cyber DBT in the nuclear sector. It will provide practical ideas on the development of a cyber threat assessment and cyber DBT along with its impact and challenges.

State

India

Gender

Male

Author: Mr PARULKAR, Sanjay Kumar

Presenter: Mr PARULKAR, Sanjay Kumar

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