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

S. K. PARULKAR,
Ex-BHABHA ATOMIC RESEARCH CENTRE, MUMBAI, INDIA
Email: parulkarsk@gmail.com

Abstract

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:

- Cyber threats are a global phenomenon not only local.
- It is not possible to know all the cyber adversaries, as they are spread all over the globe and not open or known in public as in physical adversaries.
- No intelligent agencies can find out their characteristics like capabilities and intensions, as they are not open or known.
- Cyber adversaries are location independent as they can attack from any where in the globe, which makes the task of intelligent agencies further difficult.
- 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.
- 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.
- 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***.
- Cyber resources used in attack are easily available in the open market without any restriction and can be purchased without any issue and may not required large funds as compared to physical resources.
- Even if cyber adversary caught he may not be coming under the jurisdiction of legal framework of the country where attack has occurred. Therefore the cyber adversary can not be punished.

Points 6,7,8 and 9 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 derive 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.

Keywords: detection, threat, assessment, DBT, attack, vulnerability, exploits.

1. INTRODUCTION

Nuclear facilities depend on information technology and information systems to successfully carry out their missions and business functions and processes. Information systems of nuclear facilities are as simple as office networks, financial and personnel systems to very specialized systems like industrial/process control systems, weapons systems, telecommunications systems, NMAC and environmental control systems.

Information systems of nuclear facilities are subject to serious cyber *threats* that can have adverse effects on facilities operations and assets, individuals, other organizations, and the Nation by exploiting both known and unknown *vulnerabilities* to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems
Information systems play an essential role in all aspects of the management and safe and secure operation of nuclear facilities, ***including physical protection.*** Information systems are being deployed at many Nuclear Facilities to perform various functions associated with Safety and Security of the facility. Cyber threat to such information systems are also growing world-wide in multiple dimensions. It is vitally important that all such systems are properly secured against malicious intrusions. Therefore, securing information systems against such cyber threats has become a significant component in nuclear security.

Robust cyber security has to be seen from both proactive and reactive approaches. In reactive approach, facilities actively monitoring developments in new malware and its ecosystems and have mature processes for dealing with malware and other threats found in information systems environment. Traditionally nuclear facilities are implementing reactive approach for designing and planning security protections for information systems. Proactively, facilities pay close attention to the adversarial threats that might target facility assets, areas where they are active, and trends and developments in their methods. This approach enables the facilities to better allocate finite defensive resources in the most effective manner.

In proactive approach it is essential to evaluate a workable or more practical methodology for cyber threat assessment and cyber DBT to get the credible and more realistic cyber adversarial threats, which can be used to evaluate cyber risk on nuclear facilities information systems. Based on the risk on information systems facilities design the effective cyber protections using graded approach.

It is essential to analyze threats to information systems of nuclear facilities by rigorous cyber threat assessment and subsequently deriving cyber DBT

2. BRIEF DESCRIPTION OF CLASSICAL METHOD OF THREAT ASSESSMENT AND DBT (NSS 10 DOCUMENT)

In NSS 10 document the evaluation of DBT is described in two following stages:

- Threat assessment;
- The screening and decision making process to evaluate DBT.

2.1 The first stage: Threat Assessment

The threat assessment is a comprehensive compilation of information about all potential adversaries along with their motivation, intentions and capabilities. Once the information has been collected, the data are analyzed to identify and document the credible motives, intentions and capabilities of the potential threats. This document provides as much detail as possible about threats and their credibility.

2.2 The second stage: Evaluation of DBT

To evaluate the DBT the threat assessment document is processed ***through screening and decision-making***. The main purpose of the processing is to make threats in threat assessment document ***more realistic and credible for nuclear facilities. In other words to find out more likelihood threats for nuclear facilities that can be used for developing information security protection systems for highest security assurance.***

The analysis and decision making process is described in three phases (NSS 10):

- Screening the threat assessment document for motivation, intention, and capability to commit a malicious act;
- Translating the screened threats into a statement of representative attributes and characteristics of the postulated adversary;
- Modifying the statement of representative threat attributes and characteristics on the basis of relevant policy considerations.

2.2.1 Phase 1: Screening the threat assessment document

The screening of threat assessment is carried out in two steps:

2.2.1.1 Step A: Review of capabilities

The threats described in the threat assessment document are reviewed to determine whether or not they possess the capabilities necessary to commit a malicious act that could lead to unacceptable consequences. If the capabilities of the threat are not sufficient to cause these unacceptable consequences, then that threat is discarded from further consideration for the DBT. **It is presumed that these threats are not credible or realistic for the facilities.**

2.2.1.2 Step B: Review of motivation and intentions

The threats from Step A are further screened for their motivation and intentions. If the threat, in addition to having sufficient capabilities, is also believed to have sufficient motivation (or actual intention) to commit the malicious act, then this threat is retained for further consideration in Phase 2 of the process. If neither motivation nor intent is present, the threat is a candidate for exclusion. **It is again presumed that these threats are also not credible or realistic for the nuclear facilities.**

The output of phase 1 is a **modified threat assessment document** that includes the range of credible and realistic threats that is capable and may be motivated or may have the intention to commit a malicious act leading to unacceptable consequences.

2.2.2 Phase 2: Translating threats in modified threat assessment document into representative adversary attributes and characteristics

The threat descriptions from Phase 1 are translated into a set of representative adversary characteristics that are representative of the specific ones.

2.2.3 Phase 3: Modifying representative adversary attributes and characteristics on the basis of policy factors

The representative adversary characteristics from Phase 2 are assessed for relevant policy factors to adjust the representative adversary characteristics to enable levels of security to be made more sustainable and provide balance against the costs of protection and the risks of the consequences of a potential malicious act.

3. ISSUES WITH CLASSICAL CYBER THREAT ASSESSMENT AND CYBER DBT

The classical methodology described in NSS 10 document for Physical threat assessment and physical DBT may not be sufficient to describe all the cyber threats (Adversaries) due to a few differences in physical and cyber threats as described below.

The classical threat assessment process starts with the identification of adversaries around the location of the nuclear facility. This is very much possible in physical adversaries and physical threats by the intelligent agencies but cyber adversaries are most of the time hidden in the cyber space. The cyber space is whole glob not limited only the location of the nuclear facility. No intelligent agencies can find out all the possible cyber adversaries that are active in whole glob at the same time it is very impractical for any intelligent agency to get full list of cyber adversaries in the location of the nuclear facility. In any cyber event facility only know that the event is cyber event but normally not able to catch the cyber adversaries responsible for the cyber event. **So it is very confusing for the State how to start the cyber threat assessment process where it is not possible to get the full list of cyber adversaries.**

As it is not possible to have a comprehensive list of cyber adversaries, National intelligent agencies cannot find out cyber adversary characteristics (Capabilities, Motivation and Intentions). Even if the adversaries are known, their characteristics (especially capabilities) may change in extremely dynamic manner, without getting noticed by the member state. **Without knowing cyber adversaries and their characteristics cyber threat assessment process becomes more confusing for the State using classical methodology described in NSS 10 document.**

In classical threat assessment methodology, it is difficult to know the cyber adversaries and their characteristics like motivation, intention and capabilities. Therefore the three phase processing to derive cyber DBT using threat assessment document also fails, as the main purpose of the processing is to get more credible and realistic (Likelihood) threats and their characteristics by reviewing motivation, intention and capabilities of the adversaries and further adjusting these characteristics for sustainability and cost effectiveness. When it is not possible to get the comprehensive list of cyber adversaries and their characteristics, State cannot rely on this methodology for cyber threat assessment and cyber DBT.

4. SUGGESTED APPROACH FOR CYBER THREAT ASSESSMENT AND CYBER DBT

As it is very difficult to know the cyber adversaries physically and their capabilities, intentions and motivation are also not known, in such situations it is not possible to use classical threat assessment methodology to get cyber threats assessment comprehensively.

Guards, guns and gates cannot provide Cyber security because the cause of cyber threats is unauthorized entry of malicious information into the information systems. Cyber protection is to be provided against the unauthorized information entry into the information systems.

In new suggested methodology for cyber threat assessment, it is presumed that cyber adversaries are always actively present and they can use standard cyber attack vectors in different combinations and with various possible types of Tactics, Techniques and Procedures (TTPs) to inject malicious information into the information systems. Cyber protection has to be provided against the entry of malicious information and not to the physical existence of the adversary. However to restrict the entry of cyber adversary into the facility premises is the job of physical security, cyber protection cannot restrict the entry of cyber adversary in any way. ***So in cyber threats, it is not important who is the cyber adversary, more emphasis should be given to the possible attack vectors along with different possible types of TTPs those will be used by the cyber adversaries.***

4.1 Standard known cyber attack vectors

Cyber attack vectors are the means or road used by the cyber adversary to access a device/system/network to inject malicious information into the facility information systems, for the purpose of launching a cyber attack, information gathering, planting malware, etc. ***States, not having cyber threat assessment or cyber DBT, are planning cyber protections against these standard known cyber attack vectors in traditional way. This approach cannot provide enough assurance for the cyber protection of high-risk information systems. That is the reason it is necessary to work out more precisely on these standard attack vectors through cyber threat assessment and cyber DBT process***.

Several known attack vectors are as follows:

- Phishing Attacks
- Unsecured Wireless Networks
- Removable Media
- Mobile Devices
- Malicious Web Components
- Viruses and Malware
- Supply chain
- Denial of Service (DoS) and Distributed Denial of Service (DDoS)

4.2 Suggested methodology for Cyber Threat Assessment

A cyber threat assessment is a formal process of gathering, organizing and assessing information about existing standard cyber attack vectors or possible combinations of these standard attack vectors that may be used by cyber adversaries along with different types of ***TTPs***, based on the latest technologies available, that could result in or lead to a malicious act. ***TTPs are the cyber adversary characteristics, which evaluate the skill of cyber adversaries on how cleverly they can use standard cyber attack vectors. These characteristics are the metrics to measure the capability of cyber adversary. Further, since the most of the cyber attack can spread and the systems will get infected without any specific intent or motivation by the adversary, evaluation of intention and motivation does not carry much meaning in case of cyber threats, as is the case for physical threats.***

To carryout cyber threat assessment, Competent authority of nuclear facilities can involve cyber experts from all known cyber security consortiums and cyber experts world wide to get some more standard cyber attack vectors and the different possible types of ***TTPs (Cyber adversary characteristics), based on available latest technologies*** (***cyber threats are more technology intensive***) that cyber adversary can use with standard cyber attack vectors or with combination of standard cyber-attack vectors.

The challenge is the required skill of cyber adversaries for adapting different types of cyber adversary characteristics (TTPs) along with single standard cyber attack vector or combination of standard cyber attack vectors or sometimes even with the combination of physical attack vectors that measures the capability of cyber adversaries that has to be addressed by safeguards and countermeasures (security protections) by the organization.

4.2.1 Output

A comprehensive compilation of standard cyber attack vectors or combination of standard cyber attack vectors along with different possible types of cyber adversary characteristics (TTPs) would provide a set of more effective ***cyber attack vectors***. A threat assessment document can be prepared to describe these cyber attack vectors in details specifically for nuclear facilities, that can be used to design cyber security measures as well as cyber system design for the operator. ***This should include cyber attack vectors launched from outside through networks and from direct physical access to computer system by insider***. ***If not too specific, it may not need frequent up-dates.***

4.3 Suggested method for Developing a Cyber Design Basis Threat

Development of cyber DBT can be carried out in two parts

- **Part 1.** Studying and analyzing all attack vectors along with TTPs already used in number of cyber attacks by cyber adversaries in the past.
- **Part 2.** Processing the cyber threat assessment document through further analysis and decision-making process based on relevance to the nuclear facility.

4.3.1 Part 1. Cyber DBT

There is number of cyber events taking place all over the world every year and the historical data on number of these actual cyber events (like stuxnet etc) is available in public domain. Comprehensively analyze the available historical data on past cyber events for the type of attack vectors along with different types of cyber adversary characteristics (TTPs) used in cyber event by cyber adversaries to collect all possible cyber threat vectors already utilized by the adversaries. IAEA INCIDENT AND TRAFFICKING DATABASE (ITDB) may also be utilized for this purpose.

Competent authority of nuclear facilities can involve cyber experts from all known cyber security consortiums and cyber experts' world wide to study and comprehensively compile all the attack vectors along with different types of cyber adversary characteristics (TTPs) ***used in historical cyber events all over the world. These cyber attack vectors with cyber adversary characteristics (TTPs) are very credible, realistic and authentic as the cyber adversaries' used these attack vectors in real cyber events. There is no need to prove that the cyber adversaries behind these cyber events do not have the cyber capabilities, intention or motivation as the adversaries have proved and demonstrated the same in the past. Therefore no screening is needed for capabilities, intention and motivation, as is the case in physical DBT process.***

However, a detailed document can be prepared for cyber attack vectors along with cyber adversary characteristics (TTPs) already used by the cyber adversaries. This threat vectors in the document will be further processed in part 2 of Cyber DBT under phase 2 below.

4.3.2 Part 2. Cyber DBT

The input to the development of cyber DBT process is cyber threat assessment document. This is carried out in three phases:

4.3.2.1 Phase 1: Review for capabilities:

Competent authority using appropriate stakeholders can carry out screening of cyber attack vectors for different types of cyber adversary characteristics (TTPs) listed in cyber threat assessment document for **appropriate** capabilities at the same time more relevant for the specific nuclear facility`s targets (based on facilities computer security architecture and overall facility architecture as well technology being used or any other site specific reason) for which cyber DBT Is to be prepared. These screened cyber attack vectors are the right candidates for the DBT vectors.

Using statistical analysis on specific and credible historical cyber threat data, cyber experts can find out information on various types of cyber attacks vectors, cyber attack trends and frequencies of attacks. Competent authorities can also use on top of the above, this information, to some extent, for screening more credible and realistic cyber attack vectors from threat assessment document.

4.3.2.2 Phase 2

Translate the resulting screened list from phase 1 **and from part 1 Cyber DBT above** into a statement of representative cyber threat vectors by grouping of types of cyber adversary characteristics (TTPs) of cyber attack vectors into sets of representative cyber adversary characteristics (TTPs) of attack vectors ***as ultimately organization has to design cyber protection against cyber adversary characteristics (TTPs) irrespective of the cyber adversary.***

4.3.2.3 Phase 3

Modifying the statement of representative threat vectors for relevant policy considerations. This may result in adjustments of the representative cyber threat vectors for anticipating the near future technology advancement ***to make them more sustainable*** and also against creating a balance for costs of protection and the risks of the consequences of a potential malicious act.

4.3.3 Output

The out come of phase 3 above is documented. ***As these cyber attack vectors along with types of cyber adversary characteristics (TTPs) listed in this document are more credible, realistic and authentic, it can be very well considered as cyber DBT document.***

5. BEYOND CYBER DBT

In cyber DBT document, competent authority may analyze threat vectors for which no protection can be designed or planned by the operator due to facility and information security architectures, technological constrained or any other limitations. Due to uncertainty of TTPs used in Advanced Persistent Threat (APT), it is difficult to predict and assess them. Therefore APTs are the candidate for Beyond DBT category. ***These threat vectors against which no protection is possible by the operator can be listed as beyond DBT cyber threat vectors.*** Though the protection against these threat vectors will be the responsibility of the state however operator has to help state in possible response and recovery of the information systems affected by the cyber event. In very high risk situations operator may make some arrangements with a few cyber expert teams who can help in response and recovery process.

6. RESPONDING TO NEW AND EMERGING THREATS

As cyber threats are more technology intensive and cyber technology is changing at very fast rate, new TTPs are also immerging at fast rate. In cyber threat assessment and cyber DBT, there should be some provision to accommodate these new emerging TTPs, due to technology up gradation, into threat assessment and DBT document. Subsequently these TTPs can be merged into threat assessment and DBT document during schedule revision of the respective documents.

7. CONCLUSION

The most of the nuclear facilities provide traditional cyber security protections against standard cyber attack vectors, without going through the systematic assessment of these cyber standard attack vectors and cyber DBT process. Tactics, Techniques and Procedures in utilizing standard cyber attack vectors plays an important role. Like compromising insider or getting some important information on information security systems using some procedure and tactics will enhance the capabilities of standard attack vectors. The skill to combined two or more attack vectors will enhance the capability of the adversary in multiple fold.

In an advanced persistent threat, an adversary that possesses sophisticated levels of expertise and significant resources, which allow it to create opportunities to achieve its objectives by using various types of (TTPs) along with multiple attack vectors (e.g., cyber, physical, and deception) including blended attacks. Uncertainty is particularly a major concern in APT because in such type of events, the common body of knowledge is sparse, and past behavior may not be predictive. These adversaries are having highly sophisticated skill in utilizing various types of TTPs. ***APTs are very difficult to assess in threat assessment process because it is highly unpredictable the use of TTPs in the event.***
The more relevant characteristics of cyber adversaries are TTPs and not capabilities, intention and motivation. TTPs decide the strength of cyber adversaries and cyber protections are designed and developed against the TTPs. Computer security professionals and information technology professionals can help their organizations move from traditional methodology used for information protection based on standard cyber attack vectors to a comprehensive compilation of standard attack vectors for different type of possible cyber adversary characteristics (TTPs) would enable better strategic decision-making on information protection.The outcome of classical methodology for cyber threat assessment and cyber DBT will not be different but will provide similar outcomes as above, ***if facilities can utilize it from practical point of view***. Classical methodology of threat assessment is more oriented for physical threat assessment methodology and tried to follow the same sequence of procedures for cyber threat assessment and cyber DBT. It creates more confusion when facilities try to follow classical methodology for cyber threat assessment and cyber DBT.

REFERENCES

(1) NST058 (Revision of NSS 10) DOCUMENT
NUCLEAR SECURITY THREAT ASSESSMENT, DESIGN BASIS THREATS AND REPRESENTATIVE THREAT STATEMENTS, DRAFT-IMPLEMENTING GUIDE

(2) NSS 10 DOCUMENT
DEVELOPMENT, USE AND MAINTENANCE OF THE DESIGN BASIS THREAT, IMPLEMENTING GUIDE