The Necessity of Exercise for Nuclear Facilities Considering a Blended Attack

Kim Seungmin
Korea Institute of Nuclear nonproliferation And Control(KINAC), Division of Cyber Security,
1418 Yuseong Daero, Daejeon, Korea
Corresponding author: smkim90@kinac.re.kr

1. Introduction

Based on the Enforcement Decree of the Act on Physical Protection and Radiological Emergency, Korean nuclear facilities are conducting physical protection exercise and cybersecurity exercise to verify its effectiveness and the organization's readiness to execute contingency plan [1,2]. As seen in the Russian-Ukrainian war, recent wars are being conducted as hybrid warfare that combines cyberattacks in addition to military operations. Nuclear facilities can also be the target of a blended attack that combines physical and cyberattacks, so exercise for blended attacks is necessary. The purpose of this paper is to present the method and necessity of creating a blended attack threat scenario considering cyberattacks to the existing physical protection threat scenarios.

2. Way of writing Blended Attack Scenario and Necessity of Blended Attack Exercise

Nuclear employees are conducting physical protection exercise and cybersecurity exercise based on the threat scenario reflecting the maximum threat according to the DBT (Design Basis Threat) and the response scenario prepared based on the physical protection system in the nuclear facility Currently, physical protection exercise for nuclear facilities in Korea does not consider cyberattacks, and cyber security exercise is conducted separately from physical protection exercise [3]. In this section, the characteristics of the existing physical protection and cybersecurity exercise are explained, and the blended attack threat scenario creation method that reflects the characteristics of each exercise and the necessity of exercise through the blended attack threat scenario are presented.

2.1 Feature of the Physical Protection Exercise

The main feature of the physical protection scenario is to create an ADS (Adversary Sequence Diagram). ADS is a table that determines the attacker(terrorist)'s penetration route by analyzing several intrusion paths for a target point. The final destination of the ADS is determined as a place for unauthorized removal of nuclear or other radioactive material or a place where sabotage potentially leading to unacceptable radiological consequences. Afterwards, in order to complete the ADS, the nuclear employees set the protection area of the nuclear facility and identify all the systems (i.e. fence, turn-style gate, CCTV, etc.) that the attacker in the protection area must overcome. An example of an ADS is shown in the figure below [4].

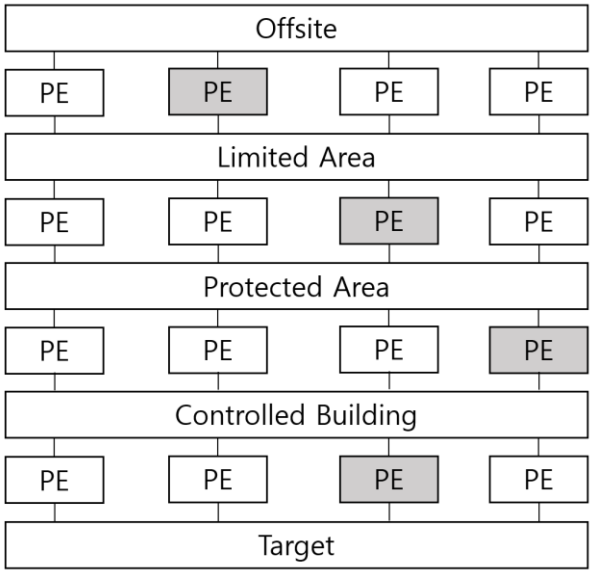

Fig. 1. Example of Adversary Sequence Diagram.

Up to the target, there are four physical areas: Offsite, limited area, protected area, and controlled building. A PE (Path Element) exists in each physical area. ADS indicates whether the attacker reaches the target by incapacitating one of the PEs located in the physical area [5].

2.2 Feature of Cybersecurity Exercise

A feature of cybersecurity exercise is that CDA (Critical Digital Asset) is selected as a target system. CDA refers to digital assets that perform SSEP (Safety, Security, and Emergency preparedness) functions among digital assets in nuclear facilities. The main content of cybersecurity exercise is that the CDA is subjected to a cyberattack according to the attack technique described in the DBT, and nuclear facility workers detect abnormal symptoms of digital assets, analyze and determine cyberattacks, isolate and recover [6].

2.3 Way of Writing Blended Attack Scenario and Necessity of Blended Attack Exercise

The purpose of security of nuclear facilities is preventing from unauthorized removal of nuclear or other radioactive material or a place where sabotage potentially leading to unacceptable radiological consequences. A threat scenario considering a blended

attack should be prepared and response exercise should be performed because there is no guarantee that an attacker will perform a physical attack and a cyberattack respectively for unauthorized removal of radioactive material and sabotage. One way to create a blended attack scenario is to consider the cyberattack in the ADS, characteristic of physical protection exercise. List the CS (Critical System) and CDA existing between the protected area of the nuclear facility, and analyze whether the CS and CDA can affect the unauthorized removal of radioactive material and sabotage should be preceded. If cyberattacks are considered for existing physical protection attacks, the detection and response time may be delayed. For example, a cyberattack may delay detection by attacking an intrusion detection system or attack an access control system to allow access to unauthorized personnel. If the response time is delayed, this increases the possibility of unauthorized removal of radioactive material and sabotage. Therefore, by performing continuous exercise based on the blended attack scenario, the response time according to the attack can be reduced, and additional physical protection facilities and countermeasures can be prepared if necessary.

3. Conclusions

This paper explains the characteristics of physical protection exercise and cybersecurity exercise, and suggests a method for creating a blended attack scenario and the need for exercise through a blended attack scenario. In order to perform blended attack exercise, identification of CS and CDA located in the path of ADS used in existing physical protection exercise should be preceded. In addition, nuclear operators should establish a systematic blended attack exercise system by providing resources for blended attack exercise.

Acknowledgement

This work was supported by the Nuclear Safety Researc h Program through the Korea Foundation Of Nuclear Sa fety(KoFONS) using the financial resource granted by t he Nuclear Safety and Security Commission(NSSC) of t he Republic of Korea. (No. 1804025)

REFERENCES

[1] Presidential Decree No.26140, “Enforcement Decree of the Act on Physical Protection and Radiological Emergency”, 2015.
[2] KINAC, KINAC/RS-015, “Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities”, 2016.
[3] INFCIRC/225/Rev.5 (IAEA Nuclear Security Series No. 13), “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities”, IAEA, Vienna, 2001.
[4] KINAC, KINAC/RS-116, “Physical Protection Exercise for the Nuclear Facilities”, 2020.
[5] M.K.Snell, SNL, “Adversary Sequence Diagram(ASD) Model”, 2007.
[6] KINAC, KINAC/RS-011, “Cyber Security Exercise for the Nuclear Facilities”, 2020.