An Overview of Nuclear Cyber Threat Assessment Framework and Analysis Cases

Subong Lee [a], Kookheui Kwon[a*], Hyunjoo Lee [a]
[a] *Korea Institute of Nuclear nonproliferation And Control, 1534 Yuseung-daro, Yuseung-gu, Daejeon, 305-348, Republic of Korea*
[*] *Corresponding author: vivacita@kinac.re.kr*

***Keywords :** Cyber Threat, Cyber Threat Assessment, Design Basis Threats, Nuclear Facilities

1. Introduction

Cyber threats are changing with the development of computer and network technologies, and if national critical infrastructures, such as nuclear facilities, are attacked, it can not only disrupt public services but also threaten the safety of the public.

To protect against such cyber threats, based on the 「Act on Physical Protection and Radiological Emergency」, cyber threats to nuclear facilities shall be evaluated to identify threats that are the basis for the design and evaluation of physical protection system, which is referred to as "Design Basis Threat (DBT)", and physical protection measures shall be implemented.

This study describes the framework of nuclear cyber threat assessment and analysis cases for evaluating the cyber threats to nuclear facilities. Furthermore, the result of nuclear cyber threat assessment will be used to re-evaluate the existing DBT.

2. Cyber Threat Assessment Framework

The cyber threat assessment consists of three main phases: data collection, screening, and analysis. In the data collection step, information about actual or possible cyber threat activity is collected. In the data screening step, the major cyber threats (actual cases) are selected from the collected cyber threat information that may have implications for nuclear facilities. In the data analysis step, major cyber threats are analyzed to identify various threat attributes, including the attack tactics, techniques, procedure, and motivation, intent used in the threat.

Cyber threat assessment is a process of collecting, screening, and analyzing threat information to identify and describe cyber threats that need to be considered from a nuclear security perspective.

2.1 Data Collection

To re-evaluate the DBT, it is necessary to systematically collect cyber threat data in domestic and abroad. Cyber threat data is collected focusing on incidents, software vulnerabilities, and technology issues for the last three years.

The scope of incidents was determined by targeting domestic and abroad industrial control-related fields with similar environments to nuclear facilities. The industrial control-related fields include manufacturing, energy, engineering, oil, gas, electronics, industrial, electricity, infrastructure, hydropower, and metals. The scope of the software vulnerability is targeted at international industry control systems (ICS). Information-sharing services are provided by the Cybersecurity and infrastructure Security Agency (CISA) can be utilized.

2.2 Data Screening

In this step, major cyber threats are selected based on their importance to the nuclear facility. There are two criteria for selecting the major cyber threats. First, some cases directly targeted the Operational Technology (OT) area including ICS will be selected because it is similar to the environment of nuclear facilities. Second, some cases that targeted the Information Technology (IT) domain were considered because attacks on the OT domain can penetrate or leverage the IT domain.

2.3 Data Analysis

In the data analysis, statistical analysis is performed on all cyber threat data to analyze overall trends. Additionally, major cyber threats are analyzed in detail using four methodologies. Table I summarizes the description of each methodology, analysis outputs, and applications.

Table I: Methodology for Detailed Analysis

Methodology	Description	Output	Application
Purdue Model [2]	A model that layers processes between IT and OT areas and divides them into levels (Level 0 to 4)	Attack Scope	Criteria for selecting major cyber threat incidents
SANS Kill Chain [3]	A model based on the Purdue model that divides the IT environment into Stage1 and the OT environment into	Attack Scope	

	Stage 2		
MITRE Threat Analysis Framework [4]	Framework for modeling and analyzing attacker tactics, techniques, and procedures (TTPs)	Attack TTPs	Information about threat attributes
Threat Attribute Classification	A comprehensive summary of threat attributes defined for this assessment	Threat Attributes	

3. Application Case

3.1 Data Collection

In this study, we collected cyber threat information for the last three years (2021~2023), focusing on incidents, software vulnerabilities, and technology issues. The scope of each cyber threat information and the collected results are summarized in Table Ⅱ.

A threat recon platform [1] operated by a specialized security company (NSHC Inc.) was utilized to collect cyber threat incidents. The information sharing service provided by the Cybersecurity and Infrastructure Security Agency (CISA) was utilized to collect cyber threat software vulnerabilities. High-powered electromagnetic pulse is selected as a technology issue that could be utilized by attackers against nuclear facilities. The results of the investigation showed that no actual cases occurred.

Table Ⅱ: Result of Cyber Treat Information Collection

Cyber Threat Information	Scope	Count Number
Incident	Domestic and international industrial control-related fields (manufacturing, energy, engineering, oil, gas, electronics, industrial, electricity, infrastructure, hydropower, metals)	175
Software Vulnerability	Vulnerabilities targeting international Industrial Control System (ICS) (CVSS score of 7 or higher, energy sector including nuclear facilities, 7 international vendors targeting nuclear facilities)	90
Technology Issue	High-powered electromagnetic waves	0
Total	-	265

3.2 Data Screening

As a result of collecting information on cyber threat incidents, SW vulnerabilities, and technology issues over the past three years, a total of 265 cases were collected. SW vulnerabilities were excluded as it is difficult to consider them as actual incidents and major cyber threat incidents were selected from 175 incidents.

A total of seven cases of major cyber threats were selected, including four cases of direct attacks in the OT/ICS domain and three cases of attacks in the IT domain. TableⅢ summarizes the selected threat cases and selection criteria.

Table Ⅲ: Cyber Threat Information Selection Results

Case	Attack Area	Criteria
EKANS Ransomware Attack [5]	IT/OT	• First ransomware to target the ICS area • Productivity reduction from ICS Attacks
Attack on Water treatment facility in Oldsmar, Florida [6]	OT	• Attacks targeted ICS area • Credential Stuffing attacks, the most common cyber-attack since 2020
Industroyer 2 Malware Attack [7]	IT/OT	• Malware attacks directly targeting the ICS area • Developed to disrupt the power grid
Pipedream Malware Attack [8]	IT/OT	• Malware attacks targeted ICS area • Designed to allow malware propagation, code modification, and lateral movement between ICS area
Solarwinds Supply Chain Attack [9]	IT	• Large-scale supply chain attacks against U.S. national organizations and nuclear organizations during supply chain attacks since 2020
Colonial Pipeline Ransomware Attack [10]	IT	• Ransomware attack on ICS surrounding systems caused a partial ICS environment shutdown • Credential Stuffing attacks, the most common cyber-attack since 2020
DOTA 3 Malware Attack [11]	IT	• Attack against domestic nation-state organizations • Credential stuffing attacks, the most common cyberattack since 2020

3.2.1 EKANS Ransomware Attack

The EKANS ransomware attack occurred in June 2020, when an unspecified cybercrime organization

attacked an Italian energy company (Enel Group) and a Japanese automobile company (Honda) for ransom. The attack disrupted Enel Group's internal network, and Honda's processes were disrupted when the ransomware spread across its internal network, exposing its automotive plants in Ohio, USA, and Turkey.

3.2.2 Attack on Water Treatment Facility in Oldsmar, Florida

In February 2021, an unspecified organization attacked a water treatment facility in Oldsmar, Florida, U.S., for sabotage. The attack was immediately discovered by an employee on duty at the time, who disconnected the attacker, and the system was restored to normal operations after the attacker was unsuccessful.

3.2.3 Industroyer 2 Malware Attack

The Industroyer 2 malware attack was an April 2022 on Ukraine's power grid by a National-sponsored organization for sabotage. The attack was scheduled to run automatically on April 8, 2022, but the Ukrainian Computer Emergency Response Team (CERT) and a security services company (ESET) with previous experience analyzing Industroyer successfully blocked the attack by proactively detecting and analyzing the malware.

3.2.4 Pipedream Malware Attack

In 2020, a Russian-sponsored organization targeted industrial control system control (CODESYS) platforms with the goal of sabotage and social disruption. Cybersecurity firms discovered Pipedream, a new attack tool against ICS, before it evolved into an attack, and worked with industrial control system manufacturer Schneider Electric to analyze and disclose the components of the attack.

3.2.5 Solarwinds Supply Chain Attack

The SolarWinds Supply Chain Attack occurred in December 2020, when a Russian-sponsored organization attacked a U.S. IT management software development company (SolarWinds) for information theft. The attack resulted in the theft of personal information and company assets of all customers using SolarWinds' network management system product (Orion).

3.2.6 Colonial Pipeline Ransomware Attack

In May 2021, the Colonial Pipeline ransomware attack was carried out by a Russian cybercrime organization (Darkside) against a U.S. oil pipeline company (Colonial Pipeline) to steal information and obtain money. The attack demanded 75 bitcoins in exchange for the decryption, which shutdown the pipeline and disrupted oil supplies in the United States.

3.2.7 DOTA 3 Malware Attack

In October 2022, DOTA 3 malware attacked the domestic nation-state institute to use it as a resource for cryptocurrency mining by a cybercrime organization (outlaw). The victim system was continuously used to mine cryptocurrency until the organization realized that it had been compromised.

4. Conclusion and Future Plan

This study describes the framework of nuclear cyber threat assessment and analysis cases for evaluating the cyber threats to nuclear facilities. Just summarized, a total of 265 cyber threats were collected from 2021 to 2023, focusing on incidents, software vulnerabilities, and technical issues, and out of 175 cyber threat incidents excluding software vulnerabilities, seven cases were defined with major cyber threats.

As a future plan, it is necessary to conduct a detailed analysis of the major cyber threats described in this paper to identify threat attributes and further analyze whether there are new threat attributes compared to the existing DBT.

REFERENCES

[1] NSHC, “사이버 위협 인텔리전스 플랫폼 ThreatRecon”, https://www.nshc.net/home/defensive-research/#ThreatRecon
[2] ANSI/ISA-95.00.01.2010(IEC 62264-1 Mod) Enterprise-Control System Integration – Part 1: Models and Terminology, ISA, 2010
[3] Michael J. Assante and Robert M. Lee, “The Industrial Control System Cyber Kill Chain”, SANS Institute, 2015
[4] The MITRE Corporation, “MITRE ATT&CK”, https://attack.mitre.org
[5] ThreatRecon, “SectorJ use Ransomware attack ICS Operations”, https://cti.nshc.net/events/view/1531, 2020
[6] ThreatRecon, “SectorJ targeted attck against a Water Treatment system in Florida, United States”, https://cti.nshc.net/events/view/2657, 2021
[7] ThreatRecon, “SectorC05 targeted cyberattack against a Ukrainian energy provider”, https://cti.nshc.net/events/view/3713, 2022
[8] ThreatRecon, “SectorJ used Malware targeted attack against a Multiple Industrial Control Systems”, https://cti.nshc.net/events/view/3722
[9] ThreatRecon, “SectorC04 supply chain attack to compromise multiple global industries”, https://cti.nshc.net/events/view/2277, 2020

[10] ThreatRecon, “SectorJ used DARKSIDE Ransomware Operations in Colonial Pipeline”, https://cti.nshc.net/events/view/2635, 2021
[11] ThreatRecon, “SectorJ used XMRig Miner targeting the vulnerable Linux servers”, https://cti.nshc.net/events/view/5918, 2022