RESPONSE FRAMEWORK AGAINST CYBER-ATTACKS AND COMPUTER SECURITY EXERCISES CONDUCTED BY NPP OPERATORS IN JAPAN

TAKIKAWA Takeshi
Nuclear Regulation Authority (NRA) Japan
Tokyo, Japan
Email: takeshi_takikawa@nsr.go.jp

Abstract

Olympic Games will be held in Tokyo in July 2020. Government of Japan has been making vast efforts to prepare for countermeasures against cyber-attacks to computer based systems and networks that control critical domestic infrastructures. Regarding protection against cyber-attacks to nuclear facilities in Japan, the NRA, regulatory body rules regulations on computer security in the NRA Ordinance and develops cyber Design Basis Threat (DBT). They are distributed to domestic nuclear licensees. Nuclear operators develop Computer Security Programme (CSP) in line with the regulation and implement protective measures in accordance with CSP. The NRA inspects all the nuclear facility operators every year in order to confirm whether those operators develop and revise CSP and implement protective measures for their computer based systems and networks in accordance with the CSP. The NRA has strengthened the computer security of nuclear facilities through these activities. This is comprehensive explanation on legal framework for cyber threat of nuclear facilities in Japan. In addition, in order to cope with actual cyber-attacks, operators need to be supported by Technical Authority. In Japan, police organization provides teams with specialized skills and resources for responding to computer security incidents. When a nuclear operator detects a cyber-attack, prompt response must be taken. And to ensure those prompt response activities are taken in a cyber-emergency, NRA requires operators to rule conducting computer security exercises regularly in operators' CSP. Some advanced NPP operators in Japan project and conduct effective computer security exercises with police organization every year. This paper provides detailed legal framework concerning computer security for nuclear facilities in Japan, the outlines of typical response framework including roles of relevant organizations when nuclear facilities' computer systems/networks are attacked and information on computer security exercises which nuclear facilities have ever projected and conducted getting cooperation and support of police organization.

1. BACKGROUND AND INTRODUCTION

Olympic Games will be held in Tokyo in July 2020. This would be one of the apparent indication that Japan is in danger of being attacked on a massive scale by cyber-criminals, crackers, hackers and like that in the near future.

Government of Japan has been proceeding preparation for cyber-attacks to computer based systems and networks which control domestic critical infrastructures. Regarding the preparation, NISC which stands for National center of Incident readiness and Strategy for Cybersecurity plays key role. NISC is an organization which was established in 2015 in Cabinet Secretariat of Japan and it represents official computer security policy and activities in Japan.

Concerning cyber-attacks launched during Olympic Games held recently, it was reported that over 200 million cyber-attacks were there on the official website of 2012 London Olympic Games during two weeks. And at the 2014 Sochi Olympic Games, it was reported 322 million cyber-attacks were there on the official website, followed by 570million cyber-attacks at 2016 Rio de Janeiro Olympic Games. It is said that tens of millions of DoS attacks and DDoS attacks were detected at 2016 Rio Olympics [1].

Under the circumstance described above, this paper will introduce three things on efforts which nuclear operators in Japan and relevant department and agency in Government of Japan are working on.

- Legal framework in Japan which is to protect computer based systems and networks of nuclear facilities;
- Computer security exercises which nuclear facility operators project and conduct with the police organizations;
- Efforts which the NRA has made and is going to make in order to establish and maintain computer security of domestic nuclear operators;

2. ORIGINALITY, COPYRIGHT AND PUBLICATION

The text of this paper is original with any material from copyrighted works included with the permission of the copyright holder. The contributor should, therefore, make sure that any permissions and rights required to publish any third-party content have been obtained and that all published material is correctly referenced.

The content of this paper have been written by the stated author and the paper itself has not been published before and be under consideration for publication by another entity.

3. CURRENT SITUATION OF COMPUTER SECURITY AT NUCLEAR FACILITIES IN JAPAN

3.1. Legal Framework in Japan

After the accident at TEPCO Fukushima Dai-ichi Nuclear Power Plant which occurred in March 2011, NISA, ex-nuclear regulatory body of Japan was reorganized and NRA was established in June 2012. About two years later in 2014, NRA provided the NRA Ordinance which includes requirements for computer security. NRA referred to publications and legislation listed below when NRA considered acts on computer security.

— NSS13（INFCIRC/225/Revision 5）[2];
— NSS17（Computer Security at Nuclear Facilities）[3];
— 10CFR/Part54 [4];
etc.

In the NRA Ordinance, two requirements are provided concerning computer security which are listed below [5].

— Uncontrolled traffic from external shall be blocked in order to protect control systems and facility security systems;
— Computer Security Programme shall be developed in order to ensure taking prompt and certain countermeasures when a cyber-attack or possibility of a cyber-attack is recognized;

NRA also made a commentary on acts concerning Physical Protection in the NRA Ordinance. It isn't made public because it contains confidential information on Physical Protection of nuclear facilities. NRA distributes it only to nuclear licensees. Secretariat of NRA made a guideline on computer security at nuclear facilities in March 2018 for the purpose of nuclear facility operators would be able to take concrete protective measures to their computer systems and networks and what they should rule in their Computer Security Programmes. This guideline is not also made public and it is distributed only to nuclear licensees.

3.2. What should be ruled in Computer Security Programme

Secretariat of NRA requires nuclear operators what they should rule in their Computer Security Programme in the guideline. Those requirements can't be noted in detail here, but most of them are based on IAEA publications listed below.

— NST045（Computer Security for Nuclear Security）[6];
— NST047（Computer Security Techniques for Nuclear Facilities）[7];

Among those requirements, Secretariat of NRA requires nuclear operators to rule conducting regular computer security exercise. And operators shall review effectiveness of their Computer Security Programme based on the results of computer security exercises and other assessments. Then if necessary operators shall revise their Computer Security Programmes properly.

4. COMPUTER SECURITY EXERCISES NUCLEAR OPERATORS CONDUCT

4.1 Purpose of computer security exercises

Comprehensive purpose of computer security exercises which Secretariat of NRA indicates nuclear operators is that operators would find issues on their protective measures of their computer systems/ networks and on their Computer Security Programmes through the exercises. Then review and improve their Computer Security Programmes and computer security. Some nuclear operators conduct computer security exercises approximately once a year in line with the purpose.
However, for those operators which have not conducted sufficient exercises so far, purpose of their computer security exercises tend to be confirming initial actions which are to be taken when a cyber-attack or possibility of a cyber-attack is detected.

4.2 Roles of relevant organizations in a cyber-emergency

IAEA publication TDL-005 (Computer Security Incident Response Planning at Nuclear Facilities) [8] shows a concept of “Technical Authority” in response entities that cope with a cyber-attack. In Japan, police organization plays roles of Technical Authority. To be correct, there are two kinds of Technical Authority in police organization. One is in local police headquarters which are located every prefecture, and the other is in National Police Agency (NPA) of Japan. Every local police headquarters has a cyber-crime inspection section and when nuclear facilities notify the police that their computer systems/networks are being attacked, cyber-crime inspection officers immediately leave local police headquarters for the facility with forensic devices and start inspection. NPA is an organization which unifies local police headquarters and it is in Tokyo. It organized 13 cyber-attack special inspection teams and located the teams to 13 major cities in Japan in 2013. When a local police headquarters asks NPA for support on inspection of and/or coping with the cyber-attack at certain nuclear facility, the special inspection team is dispatched to the facility as soon as possible using helicopters if necessary.
When computer systems/networks are attacked at a nuclear facility, operator and/or licensee is responsible for keeping their plant safe. It is clearly mentioned in law as one of the licensee’s obligations. And when operator and/or licensee cope with the cyber-attack, skilful cyber-crime inspectors and/or cyber-attack special inspection team from police organization will support.

Some explanations should be added in order to avoid misunderstandings, operators and/or licensees ***do not*** wait for arrival of police organization members before start coping with the ongoing cyber-attacks. Generally, when malwares and/or viruses are found in certain digital gears, it is a basic countermeasure to isolate the infected gears immediately from network for the sake of preventing further infection via telecommunication lines. Most of nuclear facilities in Japan organize CSIRT for themselves and when a facility operator detects a cyber-attack, facility CSIRT members are gathered and start initial actions immediately. Especially, at NPPs in Japan, plant makers put some engineers including computer system engineers at actual site all the time and CSIRT copes with the cyber-attack taking advice from the plant maker engineers and keeps nuclear facility safe.

Concerning roles of NRA and Secretariat of NRA in a cyber-emergency at a nuclear facility, NRA just receive notifications on the cyber-attack and information on countermeasures taken and conclusion of the countermeasures from operator or licensee via facsimile. NRA doesn’t instruct operator how to cope with the cyber-attack, doesn’t dispatch computer security inspectors to the nuclear facility. Because NRA and Secretariat of NRA is regulatory body.

4.3 Computer Security Exercises conducted by operators so far

Secretariat of NRA made a guideline on computer security and distributed it to nuclear licensees in March 2018 which ensured nuclear operators to conduct computer security exercises regularly. However, prior to the guideline was distributed, some NPP operators voluntarily have planned and conducted computer security exercises getting cooperation and support of police organization approximately once a year since around 2015.

At the beginning of those computer security exercises, most of those exercises were table top exercise (TTX). And purpose of those TTX was to confirm procedure of initial response actions after detecting a cyber-attack. Recently many NPP operators conduct field exercises which deal with how to cope with cyber-attacks, what they should consider in cyber-emergency and chose countermeasures they should take. Among those NPP operators, some advanced operators develop exercise scenarios referring to the latest worldwide computer security situation and they also refer to the latest approach and technique which cyber-criminals use. Scenarios in exercises which those advanced operators conducted recently were realistic enough. It's a pity that those scenarios can't be introduced in detail, one operator has conducted blended attack exercise. Blended attack means coordinated attack that utilizes both cyber and physical measures in unauthorized act. Another some operators have conducted unannounced computer security exercises.

Regarding those computer security exercises, cyber-crime inspectors from local police headquarters and members of cyber-attack special inspection team of NPA i.e. Technical Authority participates in the exercises as players. Technical Authority not only participates in the actual exercises but also voluntarily takes part in projecting exercises. In those activities Technical Authority members provide information on actual cyber-attacks like what kind of group did those attacks, what kind on technique was used in those attacks, how could they reach attack points, who did they involve in those attacks, how to cope with those cyber-attacks if being attacked, how to avoid being attacked and so on to NPP person in charge. Through these precious information provided by Technical Authority, nuclear operators can strengthen their abilities to cope with cyber-attacks and implement effective additional protective measures to their computer systems/networks.

These cooperation and support of Technical Authority make it possible that nuclear operators keep in touch with police organization without hesitation and lead enhancing nuclear operators' sense of crisis to being attacked.

4.4 Findings through observing Computer Security Exercises

When nuclear operators conduct Computer Security Exercises, they ordinarily invite computer security inspectors of Secretariat of NRA to the exercises as observers. Each inspector observe operators' Computer Security Exercises several times a year. Through the observation, Secretariat of NRA identified good practices and findings listed below.

— Good Practices
- NPP operators' system to cope with cyber-emergency is sufficient;
- NPP operators' CSIRTs are well accustomed to initial response actions;
- Relations between NPP operators and Technical Authority are OK;
- NPP operators are aware of insider threat and cope with it;
- NPP operators get latest information on cyber-attacks from Technical Authority frequently and enhance their mind-set;

— Findings
- In most exercises, players can't operate actual control systems. So person in charge should have opportunities to confirm actual operation on actual control systems during periodic check of their nuclear plants;
- Some cyber-attacks proceed covertly like STUXNET. Operators should try to find malwares and/or viruses sent and located by attackers covertly in their control systems and/or security systems before visible incidents are recognized;
- It's a typical nature of Japanese people that believing human nature is fundamentally good. Some exercise players often looks that they think and act based on the belief.

Regarding the findings listed above and other findings refrained from listing, what NRA and Secretariat of NRA should cope with as regulatory body are as follows

- Revise the guideline reflecting improving cyber-attacks' technique and distribute it to nuclear operators without delay;
- Inspect all the nuclear operators every year sufficiently by enough number of computer security inspectors with expertise on computer security and are eligible for inspection;

5. DEVELOPMENT OF CYBER DBT BY NRA

NRA started developing cyber Design Basis Threat (DBT) and adding items concerning cyber-attacks to existing DBT around 2016. One opportunity of this activity was an IPPAS suggestion which NRA received from IAEA. NRA took IPPAS mission in 2015 and received four recommendations and suggestions as the result. One of the suggestion was DBT at that time doesn't contain items concerning cyber-attack. Corresponding to this suggestion, Secretariat of NRA started investigation and consideration. Secretariat of NRA interviewed NISC officers and NPA officers and committed investigation on the latest methods and technique of cyber-attacks as well as estimated methods and technique in the near future to certain computer system/network security consulting firm. Referring to obtained information and existing DBT contents, NRA revised DBT adding items on cyber-attacks in October 2018.

The revised DBT was distributed to nuclear licensees as most confidential information. As a result, computer security exercises projected and conducted by nuclear operators have to meet cyber DBT so cyber DBT plays a role of base line of computer security exercises. And from another view point, protective measures implemented to computer systems/networks should endure cyber-attacks based on cyber DBT. It means nuclear operators have to assess their protective measures are enough or not by themselves which will enhance nuclear operators' computer security.

6. CONCLUSION

It has been around two years since nuclear facility operators in Japan are required to conduct computer security exercises regularly by the NRA Ordinance. However, since around 2015, NPP operators began projecting and conducting computer security exercises getting cooperation and support of Technical Authority i.e. police organization. As a result, some advanced NPP operators have conducted sufficient level of computer security exercises so far.

But needless to say, cyber-attack methods keep improving rapidly and technology concerning computer/network is growing day by day. For example, unknown cyber-attack utilizing zero-day information may be launched suddenly one day, quantum computers developed in the near future may solve existing cryptographs which are used in telecommunication in seconds and make it easy to intrude into control systems, like that. So implementing protective measures for control systems and facility security systems especially isolating them from outer networks are important. While it is often said that it's impossible to protect computer systems/networks completely, preparation for cyber-emergency including computer security exercises is necessary as well as implementing protective measures.

Fortunately, it is not reported so far that nuclear facility was invaded by cyber-attacks and computer systems/networks were seriously damaged, which led release of radiological materials or theft of radiological materials. But it is desirable that IAEA share information concerning cyber-attacks including to nuclear facilities in the world and vulnerability information concerning systems/networks which nuclear facilities use via IAEA conferences and/or meetings with member states because nuclear facilities would be aimed by terrorists, activists, etc. as target.

And it would be important that IAEA member states proceed computer security countermeasures' implementation of nuclear facilities in accordance with recommendations and suggestions of IAEA publications as well as physical protection countermeasures.

REFERENCES

[1] Leah Alger, "Further cyber attacks on Olympics website could occur, says researchers", Software Testing News (2018).

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), IAEA Nuclear Security Series No. 13, IAEA, Vienna (2011).

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011).

[4] United States Nuclear Regulatory Commission, Requirements For Renewal Of Operating Licenses For Nuclear Power Plants, NRC Regulations 10 CFR Part 54, NRC

[5] Nuclear Regulation Authority, The NRA Ordinance, NRA, Tokyo (2014)

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, Draft Implementing Guide NST045

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Security, Draft Technical Guidance NST047

[8] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, IAEA, Vienna (2016).