Annals of Nuclear Energy 99 (2017) 47–53

Contents lists available at ScienceDirect

Annals of Nuclear Energy

journal homepage: www.elsevier.com/locate/anucene

Cyber security in nuclear industry – Analytic study from the terror incident in nuclear power plants (NPPs)

Hyo Sung Cho [a], Tae Ho Woo [a,b,*]

[a] *Department of Radiation Convergence Engineering, Yonsei University, 1 Yonseidae-gil, Wonju, Gangwon-do 26493, Republic of Korea*
[b] *Department of Mechanical and Control Engineering, The Cyber University of Korea, 106 Bukchon-ro, Jongno-gu, Seoul 03051, Republic of Korea*

ARTICLE INFO

Article history:
Received 9 April 2015
Received in revised form 9 September 2016
Accepted 14 September 2016

Keywords:
Nuclear power plants
Cyber security
Terrorism
Safety

ABSTRACT

The cyber terrorism for nuclear power plants (NPPs) is investigated for the analytic study following the South Korean case on December 2014. There are several possible cyber terror attacks in which the twelve cases are studied for the nuclear terror cases including the computer hacking and data stealing. The defense-in-depth concept is compared for cyber terrorism, which was imported from the physical terror analysis. The conventional three conditions of the physical protection system (PPS) are modified as prevention, detection, and response. The six cases are introduced for the solutions of the facility against the possible cyber terrorism in NPPs. The computer hacking methods and related solutions are analyzed for the applications in the nuclear industry. The nuclear security in the NPPs could be an extremely serious condition and the remedies are very important in the safe plant operations. In addition, the quantitative modeling study is performed.

1. Introduction

The nuclear terrorism has been concerned extensively following the nuclear safety. The cyber terror in the nuclear power plants (NPPs) produced many security issues from the incident which had happened on December 2014 in South Korea (Republic of Korea) (ABC, 2014; BBC, 2014; Cho, 2014; Woo and Kwak, 2015). Considering of increasing trend in terrors, the attacking on nuclear facility has one of serious situations. In the attack, it was requested that unless three reactors were closed by Christmas, people should stay away from them (BBC, 2014; Woo and Kwak, 2015). However, there was not any attack on the NPPs and other nuclear facilities in South Korea. So, this paper would like to investigate the cyber terror attacks and the related matters including the protection protocols. Furthermore, recently (March 12th) the hacker asked for the money revealing the some plant drawings and the phone conversation record between Korean president and the United Nations Secretary-General (YTN, 2015). Table 1 shows the three stages of cyber terror attack on the Korea Hydro & Nuclear Power Co. Ltd. (KHNP) (VOA, 2015; Kimb, 2015). Fig. 1 is the simplified networking system for KHNP where the reactor and internal systems are disconnected from the external system (KHNP, 2014). The geological sites of NPPs are seen in the map on Fig. 2 in which the sites are located on the south east region in Korea (NGII, 2015).

Cyber terrorism in NPPs is considered as the computer-based internet terrorism as well as the nuclear terrorism in which the potential damages could be considered. In the case of cyber terror, the psychological concerns are very higher comparing to any other physical terrors. Hence, the economic damages could increase such as the stagnations of the economic activity. As a matter of fact, the employee had suffered from the maximized alert condition during all Christmas day long. The normal life cycle of the person or other scheduled tasks were delayed or cancelled in order to concentrate on the preparations against the possible terror attacks.

2. Literature review

There are several computer virus infection incidents in NPPs which could be similar effects like the cyber terrorism on NPPs. The Microsoft SQL Slammer worm was infected on the Davis-Base NPP in 2003 (US NRC, 2003; Kim, 2014). The excessive traffic in the plant's integrated computer system network had failed the recirculation pump variable frequency drive (VFD) controllers and the condensate demineralizer controller, equipped with the dual redundant programmable logic controller (PLC) system connected to the integrated computer system network on Browns Ferry in 2006 (US NRC, 2007; Kim, 2014). In addition, the Stuxnet

[*] Corresponding author at: Department of Mechanical and Control Engineering, The Cyber University of Korea, 106 Bukchon-ro, Jongno-gu, Seoul 03051, Republic of Korea.
E-mail addresses: thwoo@cuk.edu, thw_kor@hotmail.com (T.H. Woo).

http://dx.doi.org/10.1016/j.anucene.2016.09.024
0306-4549/© 2016 Elsevier Ltd. All rights reserved.

Table 1
Stages of cyber terror attack on Korea Hydro & Nuclear Power Co. Ltd. (KHNP) (VOA, 2015; Kimb, 2015).

Stage	Content
1	Data leaks by hacker in Shenyang, China Method – Direct connection – Virtual Private Network (VPN) Used software – Retired employee's ID – Fishing mail – Virus codes Data – Personal information of employees – Contents and account of emails – Internal PC
2	Emailing to KHNP employees (about 6000) with the virus code (Dec. 9, 2014). But, attack failed Method – Virtual Private Network (VPN)
3	Data opened and threatened Method – Direct connection – Virtual Private Network (VPN)

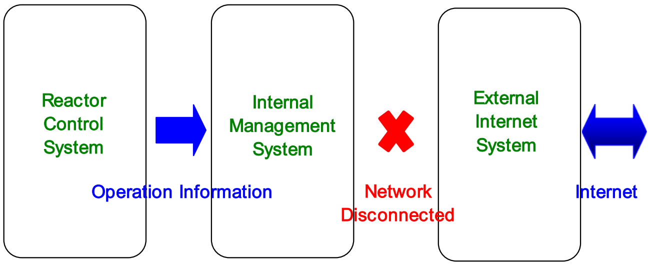

Fig. 1. Simplified networking system for KHNP.

computer worm was identified by a Belarus-based security firm (Virus-BlokAda) where Stuxnet is a serious computer virus in the NPPs (Dagouat, 2011; Kim, 2014).

Regarding the related research, the United State Department of Energy studied the cyber security in the nuclear facility for nuclear regulatory guide 5.71 (US NRC, 2010) where Title 10, of the Code of Federal Regulations, Section 73.54, "Protection of Digital Computer and Communication Systems and Networks" (10 CFR 73.54) (Ref. 1) requires, in part, that U.S. Nuclear Regulatory Commission (US NRC) licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design-basis threat (DBT), as described in 10 CFR 73.1, "Purpose and Scope."

There was the general analysis of the nuclear terror where eight cases are studied as the potential terror incidents in the commercialized NPPs (Woo, 2013a). Cipollaro and Lomonaco studied for the nuclear safety, nuclear security and nuclear safeguards (Cipollaroa and Lomonacob, 2016). Jakopič et al. studied for the quantitative verification by independent measurements (Jakopič et al., 2013). Zakariya and Kahn worked for several approaches in the design of physical protection system (PPS) (Zakariya and Kahn, 2015). In addition, there were several assessment and forecasting studies incorporated with the protection ideas (Woo and Lee, 2010, 2011a,b,c; Woo, 2011, 2012, 2013b, 2015; Woo and Kim, 2012). Shin et al. studied the nuclear cyber security issue where a risk model is based on a Bayesian network for nuclear facilities in an integrated manner (Shin et al., 2015). In addition, Silva et al. worked for making interactions in the virtual environment in which the nuclear facility structure could be simulated to give the planning action strategies to enhance its security (da Silva et al., 2015).

3. Method

The comparisons between general and cyber terror cases are shown in Table 2 where several characteristics are analyzed.

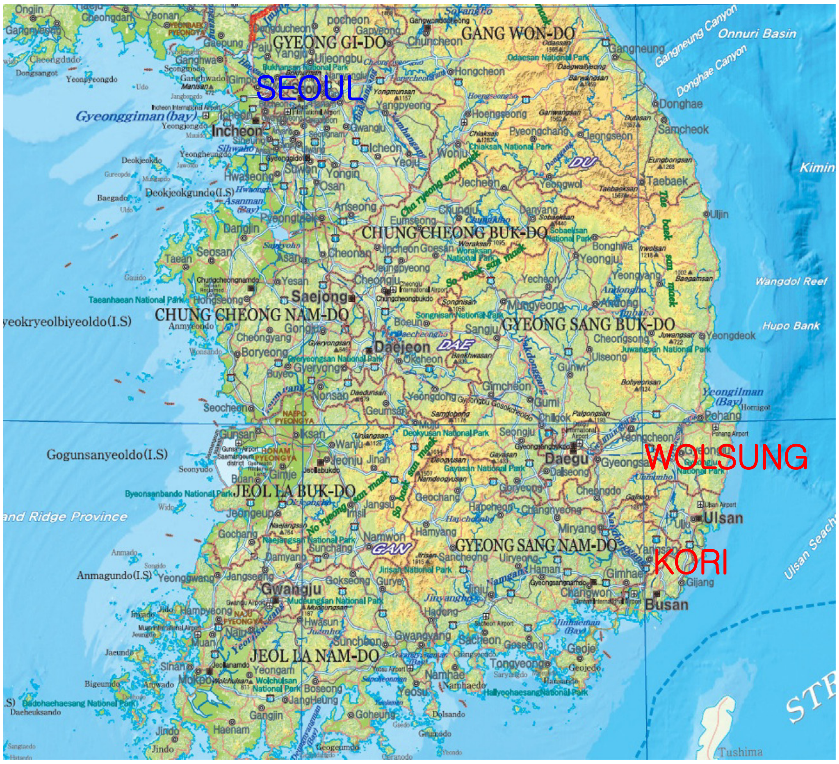

Fig. 2. Map of South Korea.

Table 2
Comparison between general and cyber terror.

	General terror	Cyber terror
Function	Detection, delay, response	Prevention, detection, response
Result	Destruction	Psychological damage, destruction
Symptom	Yes	Yes
Notice	None	Could detect
Frequency	Rare	Increasing
Preparation	Many variable systems	Networking

Table 3
Comparison between accident and terror.

	Accident	Terror
Cause	Variable	Originally human
Result	Variable	Mostly very terrifying
Symptom	Yes	Yes
Notice	None	Could detect
Frequency	Sometimes	Some cases
Preparation	Many systems from construction	Nearly none in the construction stage

Table 4
List of concepts and attacks in cyber incident (Raiyn, 2014).

Number	Type	Meaning
1	Reconnaissance attacks	Attack types by unauthorized detection mapping and service to several data
2	Access attacks	Attack with intruder gains access to the device
3	Denial of service	Intrusion in the system in order to be too busy or full to handle legitimate requests
4	Active attacks	Attack with data transmission to all parties
5	Attacks in [a]MANET	Attack with aims to slow or stop the flow of information
6	Attacks on [b]WSN	Attack by preventing the sensors from detecting and transmitting
7	Cyber crime	To exploit users for materialistic gain with computers
8	Cyber espionage	To use of internet to spy on others
9	Passive attacks	Attack with eaves dropping without meddling with the database
10	Malicious/non-malicious/attacks	Attack with intent to cause harm resulting or operational mistakes with minor loss
11	Cyber terrorism	Use of cyber space for creating large scale disruption and destruction
12	Cyber war	Act of a nation with the intention of disruption

[a] MANET (Mobile Ad-hoc Network): a continuously self-configuring, infrastructure-less network of mobile devices connected without wires (Krag and Büettrich, 2004).

[b] WSN (Wireless sensor network): a group of specialized transducers with a communications infrastructure that uses radio to monitor and record physical or environmental conditions (Rouse, 2015).

Especially, the detection possibility could be successful in the cyber terror which is particularly different from the general and physical terror case, because the Internet Protocol (IP) address is identified. However, the hacker can deceive this address for hiding any criminal activity. This kind of cyber attack is called as the spoofing attack where the attacker could avoid detection or its related degradation of the detection status (Özçelik and Brooks, 2015). Table 3 shows the comparison between accident and terror where the special differences are introduced. The clearest difference is that terror happens only by human. Otherwise, the accident could happen by variable reasons. In this study, the potential cyber terrorism consequence in nuclear facility and the treatment regarding the cyber terror incidents are discussed. This could be obtained for the modifications of the general cyber terror attack cases (Raiyn, 2014) in which the Table 4 shows the list. This list includes the general concept and the attack type together that 'cyber crime' and 'cyber war' are general concepts and 'reconnaissance' and 'denial of service' are attack types. So, the list would like to show the cyber terrorism as the terminological usages. Table 5 shows the list for possibilities in NPP facility where the cyber terror types and the meanings are discussed. As it could be possible that the synchronization of the steps is to stack to steal, the multiple concept could be mentioned in the list.

Table 5
List of possibilities in NPP facility.

Number	Type	Meaning
1	Reconnaissance attacks	Approach to the data by regular or contracted personnel
2	Access attacks	Access to the device by regular or contracted personnel
3	Denial of service	Intrusion in the system by regular or contracted personnel
4	Active attacks	Very possible by external personnel
5	Attacks in MANET	Very possible by external personnel
6	Attacks on WSN	Very possible by external personnel
7	Cyber crime	Possible by external personnel
8	Cyber espionage	Possible by external personnel
9	Passive attacks	Possible by external personnel
10	Malicious/non-malicious/attacks	Possible by external personnel
11	Cyber terrorism	Not likely possible by external personnel
12	Cyber war	Extremely not likely possible by external personnel

3.1. Reconnaissance attacks

This is a kind of common attack to the computer network. This could be happened in the external connected system. The internal network of the reactor system could not be attacked.

3.2. Access attacks

This is the virus inputting case where the non-secured area could be affected. If the site personnel intrudes into the reactor system, the system could be attacked by the virus.

3.3. Denial of service

The external network of the commuter system could be attacked by this kind of the intrusion. This is one of common cyber attacks where many experiences have been done previously like the incident of the banking systems.

3.4. Active attacks

Like the previous one, the external network of the commuter system could be attacked by this kind of the intrusion. This is one of hacking to interrupt of the normal business.

3.5. Attacks in MANET

This could be happened in the external area of the reactor building. However, the plant operation is in the serious situation, because the networking disconnection needs some time due to wireless system attack.

3.6. Attacks on WSN

Like the previous one, this could be happened in the external area of the reactor building. However, the plant operation is in

Table 6
Classification by terror attack.

Level		Characteristics	Consequence
7	Major accident	Accident	High
6	Serious accident		
5	Accident with wider consequences		Medium
4	Accident with local consequences		
3	Serious incident	Incident	Low
2	Incident		
1	Anomaly		
0	Deviation	Deviation	

Table 7
Consequence of terror attack.

Scenario	Consequence
1	Low
2	Low
3	Low
4	Low
5	Low
6	Low
7	Medium
8	Medium
9	Medium
10	Medium
11	High
12	High

the serious situation, because the networking disconnection needs some time due to wireless system attack.

3.7. Cyber crime

This could be detected by the surveillance systems before the actions. Illegal activity is treated by the international cooperation like the Interpol.

3.8. Cyber espionage

This could be detected by the surveillance systems before the actions. Spy-based computer hackings happens in many countries nowadays. The strategies are studied in many aspects.

3.9. Passive attacks

It is needed to make the secure alert in the data in order to prevent the attack.

3.10. Malicious/non-malicious/attacks

This can be detected by the surveillance system against the attack.

Table 8
Defense-in-depth by level (IAEA, 1996).

Consequence	Level	Defense-in-depth condition
Low	1	Conservative design and high quality in construction and operation
Low	2	Control, limiting and protection systems and other Surveillance features
Low	3	Engineered safety features and accident procedures
Medium	4	Complementary measures and accident management
Medium	5	Off-site emergency response

Table 9
Strategy by combinations of preventions, detection, and response (IAEA, 1996; Woo and Lee, 2011b).

Defense-in-depth condition	Strategy by combinations of prevention, detection, and response
Conservative design and high quality in construction and operation	Detection in initial stage of event regarding human factor
Control, limiting and protection systems and other Surveillance features	Detection by surveillance facility (core stability and thermal inertia, inherent plant facility like abnormal operation control system)
Engineered safety features and accident procedures	Prevention of plant damage
Complementary measures and accident management	Prevention of plant damage. Emergency response of inner-plant part
Off-site emergency response	Prevention of plant damage. Emergency response of external-plant part (External emergency response is a preventions method of accident)

Table 10
Classification of cyber terror solutions (Raiyn, 2014).

Number	Type	Meaning
1	Embedded programming approach	Some parts of the processing is performed prior to the attacks
2	Agent based approach	Servers can communicate with one another and can alarm each other.
3	Software engineering approach	The programming language with its special components will improve the programming standard
4	Artificial intelligence approach	Proposed application of the fuzzy logic concept into the cyber attack detection problem area is used
5	Cyber attack detection in cloud	Developing cyber attack detection strategy in cloud computing service environment should serve the cloud user and cloud providers
6	Cloud intrusion detection service requirements	There are a number of challenges that must be considered

Table 11
Classification of cyber terror solutions in NPP facility.

Number	Type	Characteristics
1	Embedded programming approach	Very possible and desirable
2	Agent based approach	Very possible and desirable
3	Software engineering approach	Possible to develop
4	Artificial intelligence approach	Possible to develop
5	Cyber attack detection in cloud	Possible to develop later
6	Cloud intrusion detection service requirements	Possible to develop later

3.11. Cyber terrorism

There are many defense systems which can stop the terror attacks. Usually the psychological disorders are accompanied. In this case, the significant social anomy could be spread out like the radioactive material contamination concerns.

3.12. Cyber war

This is extremely rare to be realized. However, this case is the highest damage to the society. The level of war could start the

Table 12
Classification of Korean cyber terror in NPP facility.

Classification	Content
Type (Tables 4 and 5)	Access attacks, active attacks
Consequence (Tables 6–8)	Low
Defense-in-depth condition (Tables 8 and 9)	Control, limiting and protection systems and other Surveillance features
Strategy by combinations of Prevention, detection, and response (Table 9)	Detection by surveillance facility (core stability and thermal inertia, inherent plant facility like abnormal operation control system)
Classification of cyber terror solutions (Table 10)	Urgently, number 1 and 2/Later, from number 3 to number 6

Table 13
List of modeling factor of nuclear cyber terrorism.

Factor	Value
Type	if then else(random 0 1 () < 0.3, 0, 1)
Consequence	if then else(random 0 1 () < 0.6, 0, 1)
Defense-in-depth condition	if then else(random 0 1 () < 0.5, 0, 1)
Strategy by combinations of Prevention, Detection, and Response	if then else(random 0 1 () < 0.3, 0, 1)
Classification of cyber terror solutions	if then else(random 0 1 () < 0.7, 0, 1)

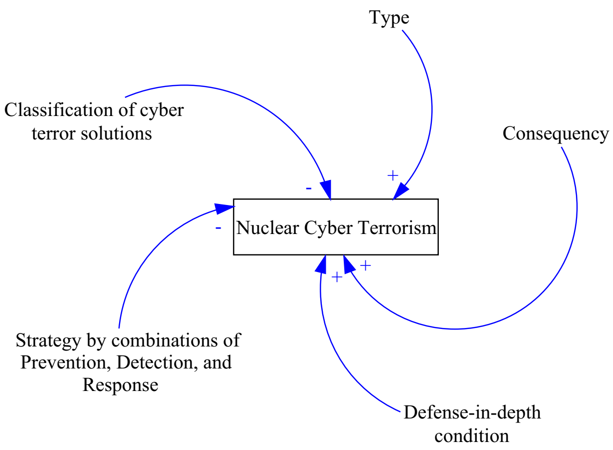
Type
Classification of cyber terror solutions
Consequency
-
+
-
Nuclear Cyber Terrorism
+
+
Strategy by combinations of Prevention, Detection, and Response
Defense-in-depth condition

Fig. 3. Modeling for nuclear cyber terrorism.

physical war using the real arms. So, this is the worst case in the proposed cyber terrors.

The above analyses are the exampled cases in which the assumptions are added to make the scenarios. Furthermore, the other kind of the cases could be imagined in the cyber systems-related terror attacks. Since there are different situation of the internet networking systems in each nation, the cyber terror possibilities have different kinds of status in the realizations of the cyber incidents.

4. Data analysis/research

The classification by possible terror attack is done by several documentations which are in Table 6 (Hagemann, 2009; IAEA, 1980, 1999, 2012; Woo and Lee, 2011b). Table 7 has the consequence list in each scenario where the subjective analyses are performed. Especially, the last one, cyber war case, is a very unlikely situation, although the terrorists could be in the situation to success in the war. There are many soluble methods which have been developed in the cyber security. There is the defense-in-depth by level in Table 8 (IAEA, 1996). This modified for the cyber terror case. That is, the strategy by combinations of prevention, detection, and response in Table 9 (IAEA, 1996; Woo and Lee, 2011b). The comparisons with the possible cyber terror cases can be quantified by the supposed level which is used in the level of the defense-in depth. There are some solutions to remedy (Raiyn, 2014) regarding the possible cycler terror attacks in Table 10 and related methods for the NPPs facility cases in Table 11.

In the case of the South Korean incident, it is classified as the cases of the Access Attacks and Active Attacks. The terrorist threatened that the NPPs would be destructed, if the operation would not stop until Christmas day. However, the disaster didn't happen due to the maximized efforts by the security agents. If the destruction happened, it is classified as Cyber Terrorism in Table 5. Furthermore, if the nation which supported the terrorist were founded out, this case is classified as the Cyber War in Table 5. Although the sorting of the incident is variable, the terrifying situation could fall the nation into the psychological disorder. Considering the case of South Korea, the concerns are extremely higher in the period of the year's end when most people are usually delight in the season. Many cerebrating schedules had been affected by the social tense mood regarding the national security. The consequence is in low of defense-in-depth condition for the Korean incident and level 2 in Table 8 where the characteristics are as the control, limiting and protection systems. The treatment for the solution is in Table 10 in which the number 1 and 2 should done urgently and then from number 3 to number 6 would be performed for the nuclear cyber security. The summary is in Table 12.

5. Modeling

The modeling for the nuclear cyber terrorism is performed where the quantitative analysis is done by System dynamics (SD) method using a software, Vensim code system (Ventana Systems, 2015). The SD has been used for the modeling simulations in the fields of engineering-technology as well as social-humanity, which was created by Dr. Jay Forrester in 1960s (System Dynamics Society, 2016). The dynamical modeling is done during 60 years calculating four times per year. The Fig. 3 shows the modeling in which five factors are analyzed in the previous chapters. The values are obtained by random number selections in Table 13. For example, in the case of Type, if the random number is lower than 0.3, it is 0.0. Otherwise, it is 1.0. Each value is summed or subtracted which are seen as plus or minus sign in the arrow line. There is the result in Fig. 4 where the dynamical values with the highest value as 3.0 at 27.75th year. There is the highest cyber terror possibility in this time, when the middle time of the operations in this modeling. This could be used in the interested NPPs for preparing against the nuclear cyber terrorism.

6. Results and discussions

In the case of the December 2014 in South Korea, although there was no significant situation, the psychological disorder was extremely high because the terrorist threatened the plant could be destructive. In addition, it was requested that all residents near site should be evacuated. However, it was not easy to catch the terrorist. According to the information, the IP address was from Shenyang, China. But, nobody knew whether the terrorist was from China, or not as soon as the incident happened. Hence, the protection preparation for the potential cyber terror attack of the future is very important. The post incident treatment could be helpless considering the speed of the incident and its related consequences.

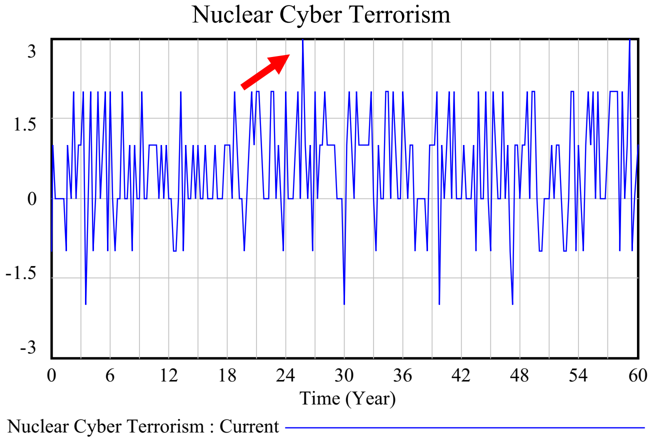

Fig. 4. Result of simulation for nuclear cyber terrorism.

This cyber terror is different from the physical terror attacks as the characteristics in which the anonymity and speed of the cyber action are much guaranteed and fast in cyber world. Although the investigation could find out the terrorist, the criminal behavior is not shown clearly. There are some solutions for preventing cyber terrors using analyzing previous terror incidents in which the radiation control is one of the most important matters. In addition, the quantitative modeling study is performed, which could be applied to the interested NPPs.

It is also important to prepare for the possible incident in which the training and surveillance are very important. The national defense system should be related with the cyber information control agency. Some nations have the training programs to produce the cyber war troops where the strategic skills are trained for the defensive as well as offensive methods. In fact, the cyber war is fearful as much as the classical war. If the NPPs are in emergency condition by cyber terror attack, it is imaginable the plant situation could be similar to the severe accident where the core melting would be happened. In this case, the radioactive material dispersions to the environment also could be imaginable. The best strategy for preventing the cyber terrorism in NPPs is to manage the information of the NPPs effectively in which the secured information controls should be guaranteed. The information from and to the NPPs should be secured. Then, the safe operation of the NPPs can be achieved. Therefore, it is necessary to make a new concept in the advanced nuclear energy development. For example, in the generation 4 (GEN-4) development strategy, the cyber security system could be installed. That is to say, the protocol for the security system is installed as the importance as much as the conventional safety features. Although the cost for the equipment would be increased, the stability of the operation could be enhanced and the expected total costs are not high considering the potential damages. Additionally, the civilian and governmental combinational preparations should be considered in the protocol construction where the commercialized NPPs and political regulations are considered simultaneously. The training for the anticipated incident is another kind of the best strategy for the preparation.

7. Conclusions

The cyber terror in nuclear facility is another kind of terror attack method. Although the reality of terrorist or object is not seen easily, the operation of the system is going to be in dangerous situation and then eventually to be in the destructive status. There are some significant points in the study as follows,

- The cyber terrorism in NPPs of South Korea shows the study motivations.
- Analyses of the cyber terrorism in NPPs are investigated.
- Designed solutions for the cyber terrorism in NPPs are discussed.
- South Korean case is considered as the cyber terrorism in NPPs.

On the cyber terror in South Korea, despite non-significant result, the psychological matter was extremely severe. Regarding of the post incident treatment, the radiation control is one of particular factors in the possible nuclear cyber terror incidents. Hence, it is needed to keep the high standard in the radioactive material managements. For the future preparations, the training and surveillance are much more important of the integrity of the nuclear facilities. In the new type system like the GEN-4 brand reactors, the cyber security defense system could be installed as the protocol or regulation of the operations.

References

ABC, 2014. South Korea seeks China's help in probe of cyber attack on nuclear power plant operator. <http://www.abc.net.au/news/2014-12-24/south-korea-seeks-china-cooperation-in- cyber-attack-probe/5988046>.

BBC, 2014. S Korea seeks Chinese help over nuclear cyber-attack. <http://www.bbc.com/news/world-asia-30596605>.

Cho, M., 2014. South Korea Seeks China's Cooperation in Probe into Cyberattack on Nuclear Operator. Thomson Reuters, New York, USA. <http://www.reuters.com/article/2014/12/24/us-northkorea-cybersecurity-nuclear-idUSKBN0K20DT20141224>.

Cipollaroa, A., Lomonacob, G., 2016. Contributing to the nuclear 3S's via a methodology aiming at enhancing the synergies between nuclear security and safety. Prog. Nucl. Energy 86, 31–39.

da Silva, M.H., Santo, A.C.do E., Marins, E.R., de Siqueira, A.P.L., Mol, D.M., Mol, A.C.de A., 2015. Using virtual reality to support the physical security of nuclear facilities. Prog. Nucl. Energy 78, 19–24.

Dagouat, C., 2011. Stuxnet Part II: Technical Analysis. ACTU SECU 27, XMCO.

Hagemann, A., 2009. DBT-Basis for Developing a European Physical Protection Concept, Office of Nuclear Security, Department of Nuclear Safety and Security, <http://www.eurosafe-forum.org/files/pe_191_24_1_5_10paper.pdf>.

IAEA, 1980. Convention on the Physical Protection of Nuclear Material, INFCIRC/Rev. 1, Vienna.

IAEA, 1996. Defense in Depth in Nuclear Safety, INSAG-10. A Report by the International Nuclear Safety Advisory Group.

IAEA, 1999. The Physical Protection of Nuclear Material and Nuclear Facilities INFCIRC 225, Rev. 4 (Corrected), Vienna.

IAEA, 2012. INES (The International Nuclear and Radiological Event Scale User's Manual) 2008 Edition (Revised).

Jakopič, R., Sturm, M., Kraiem, M., Richter, S., Aregbe, Y., 2013. Certified reference materials and reference methods for nuclear safeguards and security. J. Environ. Radioactivity 125, 17–22.

KHNP, 2014. Government united investigation committee, Recognized that the "nuclear control system is in secure" from the cyber threaten, Korea Hydro & Nuclear Power Co., Ltd. (KHNP) blog. Dec. 30, 20114.

Kim, D.-Y., 2014. Cyber security issues imposed on nuclear power plants. Ann. Nucl. Energy 65, 141–143.

Kimb, 2015. Article in March 18, 2015, Kukminilbo, Seoul, Korea, <http://news.kmib.co.kr/article/view.asp?arcid=0922999814&code=11131900>.

Krag, T., Büettrich, S., 2004. Wireless Mesh Networking, <http://archive.oreilly.com/pub/a/wireless/2004/01/22/wirelessmesh.html>.

NGII, 2015. The Map of Korea, Nation Geographic Information Institute (NGII), <http://www.ngii.go.kr/kor/popup/korea_map_200.html>.

Özçelik, I., Brooks, R.R., 2015. Deceiving entropy based DoS detection. Comput. Security 48, 234–245.

Raiyn, J., 2014. A survey of cyber attack detection strategies. Int. J. Security Appl. 8 (1), 247–256.

Rouse, 2015. Wireless sensor network (WSN), <http://searchdatacenter.techtarget.com/definition/sensor-network>.

Shin, J., Son, H., Khalilur, R., Heo, G., 2015. Development of a cyber security risk model using Bayesian networks. Reliab. Eng. Syst. Saf. 134, 208–217.

System Dynamics Society, 2016. Introduction to System Dynamics, Albany, USA, <http://www.systemdynamics.org/what-is-s/>.

Us, N.R.C., 2003. NRC Information Notice 2003-14: Potential Vulnerability of Plant Computer Network to Worm Infection. US Department of Energy, Washington, USA.

Us, N.R.C., 2007. NRC Information Notice 2007-15: Effects of Ethernet based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations. US Department of Energy, Washington, USA.

US NRC, 2010. Cyber security programs for nuclear facilities, Regulatory guide 5.71, US Department of Energy, Washington, USA.

Ventana Systems, 2015. Vensim software, Ventana Systems, Inc., Harvard, USA, <http://vensim.com/vensim-software/>.

VOA, 2015. Article in March 17, 2015. Voice of America (VOA), Washington, D.C., USA, <http://www.voakorea.com/content/article/2683451.html>.

Woo, T.H., 2012. Nuclear safeguard assessment in nuclear power plants (NPPs) using loss function with modified random numbers. Ann. Nucl. Energy 43, 1–7.

Woo, T.H., 2013a. Analytic study for physical protection system (PPS) in nuclear power plants (NPPs). Nucl. Eng. Des. 265, 932–937.

Woo, T.H., 2013b. Systems thinking safety analysis: nuclear security assessment of physical protection system in nuclear power plants. Sci. Technol. Nucl. Installations 2013, 1–5 (Article ID: 473687).

Woo, T.H., 2015. Nuclear safeguard protocol (NSP) construction of energy policy in nuclear power plants (NPPs) for secure power production. Energy Sources Part B: Econ. Planning Policy 10 (1), 91–102.

Woo, T.-H., 2011. Dynamical nuclear safeguard investigations in nuclear materials using analytic pair values. Ann. Nucl. Energy 38 (9), 1916–1923.

Woo, T.-H., Lee, U.-C., 2010. Modeling of operational safeguard for power productions in the nuclear power plants (NPPs). Energy Explor. Exploit. 28 (6), 433–449.

Woo, T.-H., Lee, U.-C., 2011a. Safeguard management for operation security in nuclear power plants (NPPs). Ann. Nucl. Energy 38 (2–3), 167–174.

Woo, T.-H., Lee, U.-C., 2011b. Safeguard assessment for life extension in nuclear power plants (NPPs) using a production function. Nucl. Eng. Des. 241 (3), 826–831.

Woo, T.-H., Lee, U.-C., 2011c. Safeguard assessment in nuclear power plants (NPPs) operations using analytic hierarchy process (AHP) and production function. Energy Explor. Exploit. 29 (3), 337–356.

Woo, T., Kim, Y., 2012. Technological assessment of national nuclear fuel cycle using transmutations of high-level nuclear waste (HLW). Energy Environ. 23 (4), 587–598.

Woo, T.H., Kwak, S.M., 2015. Social networking-based simulations for nuclear security: strategy assessment following nuclear cyber terror on South Korean nuclear power plants (NPPs). Ann. Nucl. Energy 81, 91–97.

YTN, 2015. Article in March 12, 2015, YTN, Seoul, Korea, <http://www.ytn.co.kr/_ln/0102_201503121558304684>.

Zakariya, N.I., Kahn, M.T.E., 2015. Safety, security and safeguard. Ann. Nucl. Energy 75, 292–302.