Contents lists available at ScienceDirect

Annals of Nuclear Energy

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

Social networking-based simulations for nuclear security: Strategy assessment following nuclear cyber terror on South Korean nuclear power plants (NPPs)

Tae Ho Woo *, Sang Man Kwak

Systemix Global Co. Ltd., 3 F, 494-48, Yonggang-dong, Mapo-Gu, Seoul 121-876, Republic of Korea

ARTICLE INFO

Article history:
Received 12 January 2015
Received in revised form 9 March 2015
Accepted 18 March 2015
Available online 2 April 2015

Keywords:
Cyber terror
Social networking circle by system dynamics diagram (SNCSD)
Social networking service (SNS)
System dynamics (SD)
Vensim

ABSTRACT

Nuclear energy has been studied for the secure power productions, which is based on the simulation study following the incident of nuclear cyber terror attack on South Korean nuclear power plants (NPPs). The social networking is used for the terror incident modeling and its prevention strategies. The nuclear industry could be investigated in the aspect of minimizing the dangerous situations caused by possible terror attacks which are considered by the society oriented connectivity among the related people or groups. The social networking circle by system dynamics diagram (SNCSD) is constructed, where the configuration of a model social networking example by system dynamics (SD) is applied. From *A* to *H* regions, the values are obtained by the random numbers incorporated with the designed algorithms. The results show the comparative values of terror possibilities which are based on the proposed social networking algorithm. It is possible to prepare for potential terrorism in the nuclear industry.

1. Introduction

The social network theory has been applied to the terror prevention in nuclear energy production following the nuclear cyber terror attack on the South Korean nuclear power plants (NPPs) happened on December 2014 (Republic of Korea) (ABC, 2014; BBC, 2014; Cho, 2014). The designs and manuals of plant equipment owned by Korea Hydro and Nuclear Power Co (KHNP) were put online by an unknown individual or group (BBC, 2014). The threat was unless three reactors were closed by Christmas day, people should “stay away” from them (BBC, 2014) and fortunately there was not any attack on the NPPs and other nuclear facilities in South Korea. Table 1 shows the list of cyber terror attack for Korea Hydro & Nuclear Power Co. Ltd. (KHNP) (Energy Justice Actions, 2015; Pressian Coop., 2015; Yonhapnews, 2014). It is important to make the secured operation through the assessment of the incident which would be applicable for the terror prevention strategy.

Networking in this study has the characteristics of connection between the terror event related persons. The 9/11 terror is usually used for the example in the case of the terror incident targeting the civilian object. The social networking has been studied for the terror phenomenon and its prevention strategy suggestions. Hence the nuclear industry could be investigated in the aspect of minimizing the dangerous situation against possible terror attacks which are considered by the society oriented connectivity among the interested people or groups. Recently, the threaten possibility of terror incident has increased in many areas. Especially, the public place like the airplane or train is very liable to be attacked by the terrorist. The NPPs are also to be wreaked against the possible terror of unknown individuals or groups. So, it is important to prepare for the possible terror attack. The social networking is one of important method to control terror incident which is analyzed in this study.

There are examples of social networking analyses to the 9/11 terror case (Fellman and Wright, 2003; Jonas and Harper, 2006; Keefe, 2006; Krebs, 2008; Morselli et al., 2007; Sageman, 2004). These studies show the networking has one of major characteristics in the incident like the terror. Fig. 1 shows the simplified networking by the mobile phone for the social networking service (SNS) where lots of information make the networking. The common method for the communications is the mobile phone-based social networking. That is to say, the invisible electronic telecommunications of information construct the networking around our lives as social structures. This SNS is very important for preventing the possible terrors in the meaning to find the clue of the terror

* Corresponding author. Tel.: +82 2 831 8394; fax: +82 2 831 8422.
E-mail address: thw_kor@hotmail.com (T.H. Woo).

http://dx.doi.org/10.1016/j.anucene.2015.03.016
0306-4549/© 2015 Elsevier Ltd. All rights reserved.

Table 1
List of cyber terror attack for Korea Hydro & Nuclear Power Co. Ltd. (KHNP).

Number	Date	Content
1	December 9, 2014	Emailing to KHNP employees with the virus code
2	December 10, 2014 at 6 PM	AhnLab (Korean computer vaccine provider company) announced the virus of MBR (master boot record) destruction and notifying "Who Am I?"
3	December 12, 2014	The press reported the incident
4	December 15, 2014	The hacker enrolled the files in NAVER blog. The leaked files were the personal information descriptions of the KHNP employees and the explanations of CANDU control program
5	December 17, 2014 around 9 PM	The hacker enrolled the sentence of cyber terror matter in NAVER blog
6	December 17, 2014	The press reported 10,779 employees information was leaked
7	December 18, 2014 around 2 PM	The hacker enrolled the files in NAVER blog. The leaked files are as follows: – AUX. Building Chilled Water drawing in Kori Unit #1 – Moderator ISO drawing in Wolsung Unit #1 – Capture scene of resident radiation estimation program around plant site (K-DOSE 60 Ver. 2.1.2) – Letter to the Crown Prince of the United Arab Emirate by South Korean President Park – Insisted that they sent 16,250 virus files
8	December 18, 2014	KHNP reported the leaked files were from external network systems. So, the operations is in secured situation
9	December 18, 2014 around 7 PM	The blog was closed
10	December 18, 2014	KHNP reported this incident was assigned to the Seoul District Public Prosecutor's Office
11	December 21, 2014	The hacker enrolled the files in NAVER blog. The leaked files are as follows: – Documentations in Kori Unit #2 and Wolsung Unit #1 – MCNP5 and BURN4 code manual – Requested to stop the operations of the Kori Unit #1 and 3, Wolsung Unit #2 during 3 months from Christmas day
12	December 25, 2014	Nothing happened to nuclear power plants on Christmas day
13	December 28, 2014	KHNP president announced the hacking attacks on KHNP were continuing with several kinds of types. But, the internal networking of reactor and its related control systems were in safe and secured condition due to manual operation system in the case of emergency

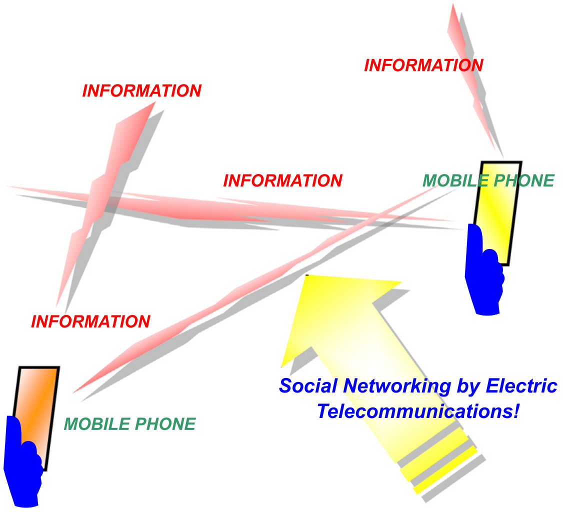

Fig. 1. Simplified networking by mobile phone for social networking service (SNS).

Table 2
Nuclear power plants world-wide in operation (28 August 2014).

Country	Number of unit	Country	Number of unit
Argentina	3	Mexico	2
Armenia	1	Netherlands	1
Belgium	7	Pakistan	3
Brazil	2	Romania	2
Bulgaria	2	Russia	33
Canada	19	Slovakia Rep.	4
China	22	Slovenia	1
Czech Rep.	6	South Africa	2
Finland	4	Spain	7
France	58	Sweden	10
Germany	9	Switzerland	5
Hungary	4	Taiwan, China	6
India	21	Ukraine	15
Iran	1	U.K.	16
Japan	48	U.S.	100
Korea, Rep.	23	Total	437

incident. However, it is difficult to find out the exact time of terror case and the terrorist. Hence, it is necessary to construct the sophisticated and intelligent ways to detect the terrorist's action.

Currently, there are many operating NPPs which are shown as the world nuclear power generation units in Table 2 (European Nuclear Society, 2014). The nuclear industry has been confronting the attack threatening of the possible anonymous terrorist. The pre-cautious approach to the terrorist could be expressed by the characteristics of the terrors. For example, the communication contents could be the hint of the incident. In addition, the position of the communicator is important. Then, the local region of the communication is also important. So, many variables should be considered by the detection system. The illegal tapping is performed in many countries. However, this method is very difficult to use, because there are strong pressure by public groups if the fact of tapping is known to the individuals. Therefore, an indirect algorithm of this study could be effective to find out the potential terror incident.

There are some terror related studies. Arndt et al. (2005) worked that a growing body of research derived from terror management theory. Gould and Stecklov (2009) argued that terrorism raises the costs of crime and imposes a negative externality on potential criminals in which terrorism raises the costs of crime through two channels. Also, Hirschberger et al. (2010) showed that the experimental study for the death prime was performed in the aspect of the motivated significance. In this paper, Section 2 explains the method of the study. Section 3 describes results of the study. In addition, there are some conclusions in Section 4.

2. Method

2.1. The epidemic and network models

The spread of computer virus is modeled which is happened in the cyber terror method (Shehu and Kushe, 2011) where the