International Journal of Grid and Distributed Computing
Vol. 11, No. 1 (2018), pp.13-26
http://dx.doi.org/10.14257/ijgdc.2018.11.1.02

Modeling of Cyber-attack Intentions Analysis Reflecting Domestic / International Situations

Jung ho Eom

Military Studies, Daejeon University, 62 Daehakro, Dong-Gu, Daejeon,
eomhun@gmail.com

Abstract

Recently, the aspect of cyber-attack is closely related to the situation in domestic and international situations. Particularly, cyber-attacks are used as means of subjugating, coercing, and expelling opponents to achieve political goals. A cyber-attack may be a goal in itself, but it may also be used as a means to achieve other goals. In the case of North Korea, it has been used as a means of revenge to prevent Sony Pictures' release of the movie, and it is trying to turn the surveillance of neighboring countries through cyber-attacks in order not to detect the nuclear test. Therefore, when analyzing the cyber-attack's goal or intention, it is expected that it will be able to identify more accurate attack intention considering domestic / international situation. We confirmed the reliability through association analysis to identify the relationship between past cyber-attack cases and the situation. And we proposed an intention analysis indicator and a model that can predict cyber-attack intention reflecting domestic / international situation. The proposed model of cyber-attack intention analysis is composed of two analysis modules; a cyber-attack pattern analysis module and a situation reflected intention analysis module. The cyber-attack pattern analysis module identifies attack techniques and targets to predict the result of the cyber-attack. The situation reflected intention analysis module generates the situation indicators and identifies the attack intention by fusing the attack pattern derived from the cyber-attack pattern analysis module.

Keywords*: Cyber- attack, Attack Pattern, Attack Intention, Intention Analysis*

1. Introduction

Recently cyber- attacks are used to achieve the goal of the attack itself, but are also used as a means. For example, in April 2013, a massive cyber-attack on the uriminjokkiri sites and North Korean affiliate websites by Anonymous was a threat against North Korea's evil conduct. In November 2014, North Korea hacked the computer network of Sony Pictures, which produced an interview movie about Kim Jong Eun's assassination story, and leaked movie contents by hacking. It was judged as retaliation against the United States. In other words, cyber- attacks can be used as means to achieve political, military, social and economic goals. If the cyber-attack itself is a goal, it directly damages the target to be attacked [1].

Considering the situation of the country that has recently conducted a cyber-attack and the international situation, cyber- attacks are often used as a means of coercion. Coercion brings the opponent's behavior change, accompanied by threats of the use of force or exemplary methods. In other words, it is one of the strategies for reaching the opponent's behavior between the two ends of the spectrum of war involving foreign policy and military action involving the armed forces. Cyber-attacks are used as a means because they are superior to physical means in terms of

Received (October 21, 2017), Review Result (December 18, 2017), Accepted (December 28, 2017)

ISSN: 2005-4262 IJGDC

cost effectiveness, and even if they fail, they are not exposed quickly and do not have a significant impact on the attacker [2].

In this paper, we propose an intention analysis model that can determine the attacker intentions when cyber-attack is used as a means. The proposed cyber-attack intention analysis model is composed of two analysis modules; a cyber-attack pattern analysis module and a situation reflected intention analysis module. The latter analyzes the intentions of the cyber-attack by collecting and analyzing information of the domestic and international situation at the time of the cyber-attack based on the results of the attack pattern analysis. This paper organized as follows. We will describe cyber-attack as a means in section 2 and association analysis between cyber-attack and situation in section 3. We design model of cyber-attack intentions analysis in section 4, and conclude in the last section.

2. Cyber-attack as a Means

Cyber- attacks as a means are used as threats, compression, retaliation, and switch surveillance. The following table shows the types of cyber- attacks usage [2].

Table 1. The Types of Cyber- Attacks Usage

Category		Explanation
Goal		In case of the necessary expense or specification is less than physical means, or the attack is effective
Means	Threat	In case of the cost of using physical means is high, or military action is not possible due to international regulations and public opinion
	Compression	the opponent is in military superiority, but the criterion of retaliation is unclear, or the criteria of self-defense are unclear, and retaliation cannot be carried out due to domestic and international regulations
	Retaliation	unable to conduct physical military force or unwilling to expand war in response to a hostile nation’s actions
	Switch surveillance	moves away from opposite nation surveillance and attempts to conduct a massive and secret political/military action

The threat is the action of exposing cyber-attack capability advantage through cyber-attack when the cost of using physical means is high, or military action cannot be done due to international norms or public opinion. Compression is the action of allowing the opponent to accept the request of the attacker if the opponent is in military superiority, but the criterion of retaliation is unclear, or the criteria of self-defense are unclear, and retaliation cannot be carried out due to domestic and international regulations. Retaliation is a countermeasure against the actions of a hostile country, and corresponds to countermeasure like the scale of damage caused by the actions of a counterparty in the event that it cannot respond physically military force mobilization. The conditions that can be regarded as a retaliatory action should be similar to the scale of the damage caused by the actions of the hostile country and should be timely compatible with the actions of the hostile country in terms of time. Finally, switch surveillance is the action of turning opposite surveillance into a cyber- attack. When an attacker moves away from opposite nation surveillance and attempts to conduct a massive and secret political/military action, he will draw attention to the opposite nation's surveillance by restoring the damage caused by the cyber- attack. Compression and switch surveillance is often used as an asymmetric power when it is relatively lower than the military capacity of the opposite nations [1-4].

The intention of cyber- attack as a means cannot be judged only by cyber- attacks in cyberspace. It should analyze the domestic and international situation, and analyze the relationship with the opponent, and find out similar cases in the past and comprehensively judge them. Particularly in the case of North Korea, cyber- attacks are often carried out look one way and row another. For example, cyber- attacks have led South Korea to focus its surveillance on cyber- attacks, to conduct military provocation such as nuclear tests and missile launches.

3. Association Analysis between Cyber- attack and Situation

It is possible to determine whether domestic and international situation can be used as analysis factors for intention analysis of cyber- attack through an association rule analysis. It is the degree of influence of domestic and international situation on cyber- attacks or conversely the degree of influence cyber- attack on domestic and international situation.

Table 2. Summary of Association Analysis

Indicator	**Rule**	**Explanation**
Support	*P(A)*	• Probability for transactions involving A and B together • Value for overall transaction size • The higher the value, the more frequent the transaction • A measure of the importance of the rule
Confidence	*P(A,B)/P(A)*	• The probability of occurrence of item B when A occurs (conditional probability) • If A occurs, it indicates how many of the item B occurs • The higher the value, the higher the B occurrence • A measure of the confidence of the rule
Lift	*P(A,B)/P(A)·P(B)*	• Whether the occurrence patterns of items A and B are independent or associated with each other • A value greater than 1 indicates a positive association

Association rule analysis [5] is the process of finding meaningful association rules between items in data. The association rule is an analysis method that identifies for rules that can cause simultaneous occurrence of items that affect the occurrence of a specific event. It is a technique for identifying a rule in which event B occurs simultaneously when a specific event A occurs. Association analysis is also referred to as market basket analysis or affinity analysis in the sense that the relationship between the items in the customer's shopping cart in marketing. The structure of rule is if (condition A) then (result B). The indicators that indicate the usefulness of association rules are support, confidence, and lift. Support shows the frequency of the patterns in the rule. It is the percentage of transactions that contains all items in the rule. Confidence is the strength of implication of a rule. It is the percentage of transactions containing all items stated in the condition that also contain the items in result. Lift is a measure of the performance of an association rule at predicting or classifying cases as having an enhanced response.

Domestic and international situations are extracted from the events that became hot issues in the political, economic, social, and military aspects based on the time of the cyber- attack and utilized as a factor of association analysis. Since cyber-attack preparatory activities generally take 3 to 6 months or even more than 1 year, important events in the domestic and international situation are also restricted from the period of preparatory activities to the point of restoration of damage after the outbreak of cyber- attack. In this case, 3 months before and 3 months after the outbreak of cyber- attack are most appropriate. In addition, the hot issue of domestic and international situation is considered as events that can recognize the importance of the event in the media and the situation analysis report. The cyber- attack that can be a population is limited to cyber terrorism or cyberwarfare that has occurred as a semi-national entity or nation in terms of size, and the level of damage has also caused a mass loss in political, social and economic aspects.

In this research, we analyze the association strength between the domestic& international situation and cyber- attack through analysis of the association rule between the North Korea nuclear test and the cyber- attack. In this case, a population is limited to cases perceived by both the Korean government and the public as a threat to South Korea, which the North Koreans have conducted since 2006 when North Korea began a nuclear test. The period is 10 years from October 2006 to September 2016. North Korea's nuclear test was carried out six times from the first nuclear test in 2006 to the sixth nuclear test in September 2017. In this research, we use threat events from the 2nd to 5th period to extract valid data. The following table shows North Korea's threats to South Korea since October 2006 [6].

Table 3. The Representative Example of North Korea’s Threat to South Korea

Num	Date	Threats
1	Oct. 2006	First Nuclear Test
2	July 2008	Park wangja’s Murder case
3	July 2009	Second Nuclear Test, 7.7 DDoS
4	June 2010	Cheonan Boat Attack
5	Nov. 2010	Yeonpyeong Island Shelling
6	March 2011	3.4 DDoS, Key Resolve Exercise, GPS Disturbance
7	April 2011	Cyber- attack on Nonghyup Bank, NK-China Summit
8	March 2013	Third Nuclear Test, 3.20 Cyber Terror, Missile Launch
9	June 2013	6.25 Cyber- attack, Missile Launch
10	Aug. 2015	Yeoncheon Rocket Launch
11	Feb. 2016	Fourth Nuclear Test, Cyber- attack, Missile Launch
12	Sept. 2016	Fifth Nuclear Test, Cyber- attack, Missile Launch

Based on the data in the above table, when a nuclear test occurs, the occurrence probability of cyber- attack and the reliability and the strength of the probability are calculated. The nuclear test corresponds to the conditional clause and the cyber-attack corresponds to the result clause. North Korea's threat to South Korea occurred 12 times in 10 years, 5 times for nuclear tests, 7 times for cyber- attacks, and 4 times for cyber- attacks and nuclear tests. The following table shows the results of the association rule analysis.

Table 4. Result of Association Analysis between Nuclear Test and Cyber- attack

Indicator	Result	Explanation
Support	33%	• Of the total North Korean threats, 33 percent of the cases of nuclear tests and cyber- attacks occurred at the same period.
Confidence	80%	• The occurrence probability of a cyber- attack following a nuclear test is 80%.

Lift	1.37	• Because the result is greater than 1, there is a high probability that a cyber-attack will be accompanied by a nuclear test.

Support that is, the probability of a nuclear test and a cyber- attack at the same period in North Korea's threats to South Korea was 33%. In other words, one of three incidents means that a nuclear test and a cyber- attack are accompanied together. Confidence is 80% with the probability that a cyber- attack is necessarily accompanied by a nuclear test. That is, the occurrence probability of a cyber- attack after a nuclear test is very high. Because lift value is larger than 1, it can be seen that there is a strong dependency between the nuclear test and the cyber- attack.

4. An Architecture of Cyber- Attack Intentions Analysis Model

The cyber- attack intention analysis model proposed in this research is composed of a cyber- attack pattern analysis module and attack intention analysis module that reflects situation, based on a causal network [7]. Because the causal network can represent probabilistic relationships of attack, evidence, and intention, it is appropriate to apply it to the algorithm that analyzes the attacker's intention. The attack pattern analysis module classifies attack indication information collected so far to generate an attack analysis indicator, identifies attack techniques and targets based on the classified attack indication information, and predicts the result of the attack. The situation reflected attack intention analysis module inputs current political, social, economic and military situation information, and classifies them and generates situation indicators. It identifies attack intentions by fusing attack pattern analysis information derived from the attack pattern analysis module. The following figure shows an architecture of the cyber- attack intention analysis model.

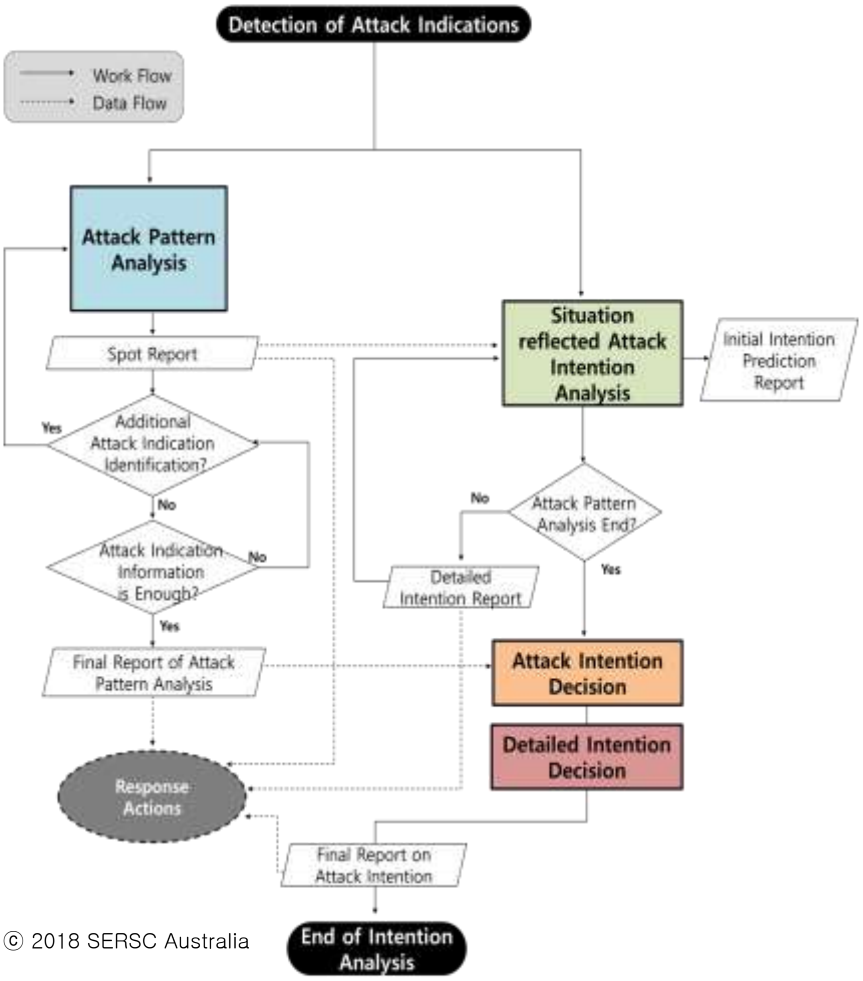
Detection of Attack Indications
Work Flow
Data Flow
Attack Pattern Analysis
Spot Report
Yes
Additional Attack Indication Identification?
No
Attack Indication Information is Enough?
No
Yes
Final Report of Attack Pattern Analysis
Response Actions
Situation reflected Attack Intention Analysis
Initial Intention Prediction Report
No
Attack Pattern Analysis End?
Yes
Detailed Intention Report
Attack Intention Decision
Detailed Intention Decision
Final Report on Attack Intention
End of Intention Analysis

Figure 1. An Architecture of Cyber- Attack Intentions Analysis Model

In the attack pattern analysis module, the analysis process is performed whenever an attack indication is identified. If an attack indication is gathered to the extent that a detailed prediction of the attack result is possible, the analysis of the attack pattern is terminated after the final report of the attack pattern analysis. The final report on attack pattern analysis is input to the process of situation reflected attack intention analysis as well as the spot report, and is also reported in the response actions system.

In the situation reflected attack intention analysis module, the intention analysis process is started after the attack pattern analysis report is inputted. This intention analysis is repeated every time an attack pattern analysis report is inputted. All processes are ended when the attack pattern analysis report is finally inputted, and the derived detailed intention is finally reported. When the analysis of the attack pattern is completed, the final attack pattern analysis report is input to the attack intention analysis process, and the enemy intention of cyber- attack is analyzed and recommended based on the contents of this report and domestic & international situation and enemy situation analysis data.

The following describes the specific procedures and methods of the attack pattern analysis module and the situation reflected attack intention analysis module.

4.1. The Attack Pattern Analysis Module

The following figure shows the concrete process of cyber- attack pattern analysis module. Attack pattern analysis analyzed attack indications and techniques of cyber-attacks that have been an issue in domestic and international over the past decade, and analyzed the attack indications and techniques that occurred before or during the cyber- attack.

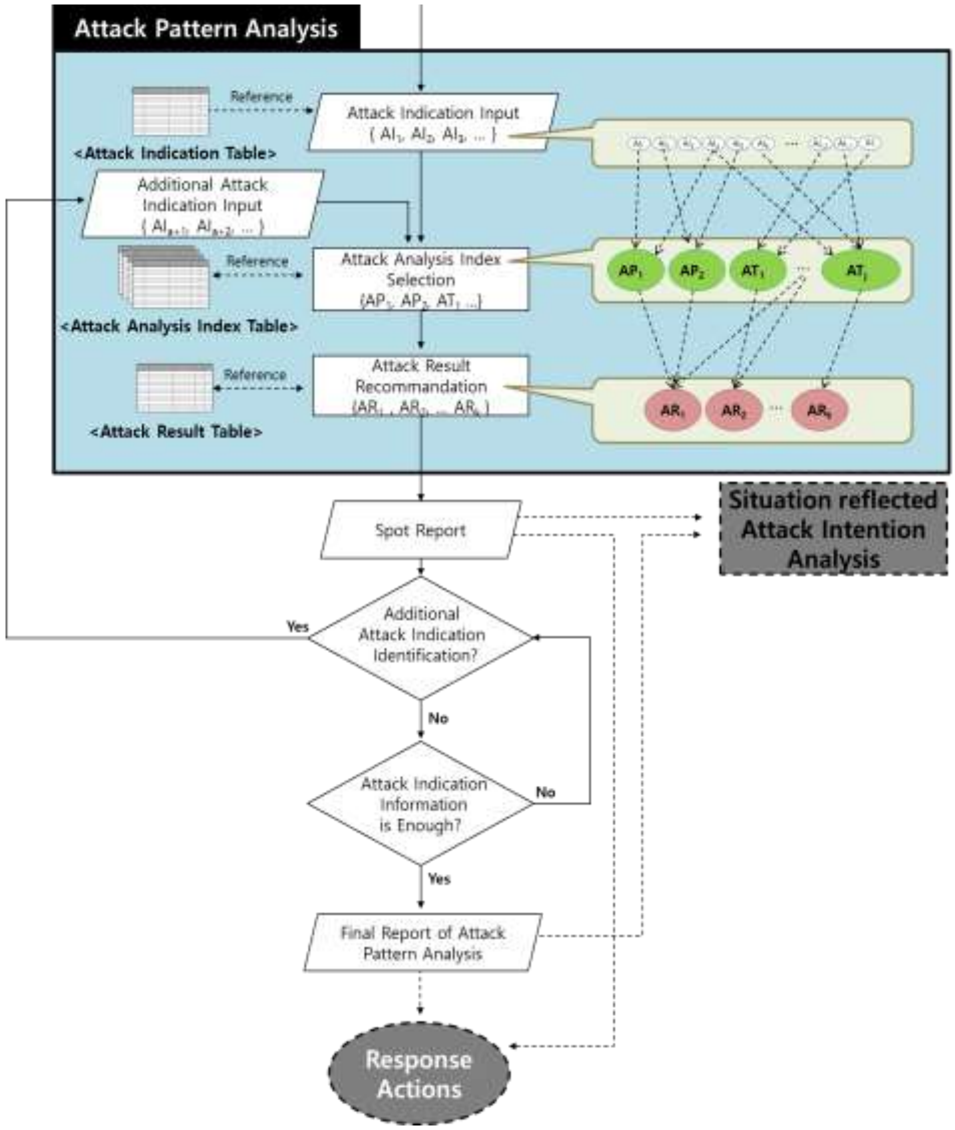
Attack Pattern Analysis
Reference
<Attack Indication Table>
Attack Indication Input (AI1, AI2, AI3, ...)
Additional Attack Indication Input (AIn+1, AIn+2, ...)
Reference
<Attack Analysis Index Table>
Attack Analysis Index Selection (AP1, AP2, AT1 ...)
AP1
AP2
AT1
ATj
Reference
<Attack Result Table>
Attack Result Recommandation (AR1 , AR2, ... ARk)
AR1
AR2
ARk
Spot Report
Situation reflected Attack Intention Analysis
Yes
Additional Attack Indication Identification?
No
Attack Indication Information is Enough?
No
Yes
Final Report of Attack Pattern Analysis
Response Actions

Figure 2. The Attack Pattern Analysis Module

The attack indication (AI) input inputs the collected attack indication information, and the indication information refers to the attack indication table like the following table. In the attack indications table, all information corresponding to the attack indications is stored, and an identification number is assigned to each indication. The attack indications are data obtained by analyzing cases of cyber- attacks over the past decade.

Table 5. An Example of Attack Indication Table

ID Number	Indications
AI0001	ICMP Ping Sweep
AI0002	TCP Connect attack
AI0003	TCP SYN Scanning
AI0004	ICMP Ping of Death attack
AI0005	XMAS Flooding Attack
…	…

The attack analysis index extraction extracts an index that accurately matches the collected indications and the indication list of the table. The indication information input in the previous process is converted into an attack analysis index by referring to the attack analysis index table. The attack analysis index table stores a list of indications that form each index. The types of attack analysis index include attack pattern and attack target, and attack analysis index table is divided into attack pattern(AP) table and attack target(AT) table like the following tables again.

Table 6. An Example of Attack Patterns Table

ID Number	Patterns	Indication List
AP13001	DDoS	AI0012, AI0052, AI0053
AP13002	DDoS	AI0013, AI0052, AI0053
AP13003	DDoS	AI0014, AI0052, AI0053
AP021004	Web Vulnerability Attack	AI0046
AP032001	Malicious Bot	AI0064, AI0052
…	…	…

Table 7. An Example of Attack Target Table

ID Number	Target	Indication List
AT11001	Server	AI0013
AT11002	Server	AI0014
AT11003	Server	AI0015
AT21001	Network	AI0012
AT31001	PC	AI0001
…	…	…

The attack result(AR) recommendation is a process of determining which attack result is expected when the attack pattern indicator converted from the attack indicator and the attack target indicator are fused. Such information is stored in the attack result table like the following table, and it is necessary to identify a record in which each converted attack index and the list of attack index in the table are exactly corresponded.

Table 8. An Example of Attack Result Table

ID Number	Attack Result	Pattern List	Target List
AR010001	Service Impossible	AP011001	AT011001
AR010002	Service Impossible	AP011002	AT011001
AR010003	Service Impossible	AP011003	AT011001
AR030001	Privacy Data Leakage	AP042001	AT061006, AT031026
AR210001	Remote Control	AP161001, AP032001	AT031020
…	…	…	…

4.2. The Situation Reflected Attack Intention Analysis Module

The following figure shows the concrete process of the situation reflected attack intention analysis module. Firstly, if attack indications are detected for the first time, the current situation information is inputted. The input to the situation information refers to the situation information table like the following table. The situation information table is consisted of 4 situations; political(PS), economic(ES), military(MS) and social situation(SS). In the situation information table, all information corresponding to the situation is stored, and an identification number is assigned to each situation information.

Table 9. An Example of the Situation Information Table

ID Number	Situations
PS0001	Nation A converts hard policy to nation B
PS0002	Announce economic sanctions policy for nation A
…	…
ES0001	The rise of international economic influence of nation A
ES0002	National economic crisis situation
…	…
MS0001	Nuclear experimentation of nation A
MS0002	Long-range missile experiment in nation A
…	…
SS0001	Social movement development in S within nation A
SS0002	Emotional conflict between nation A and nation B
…	…

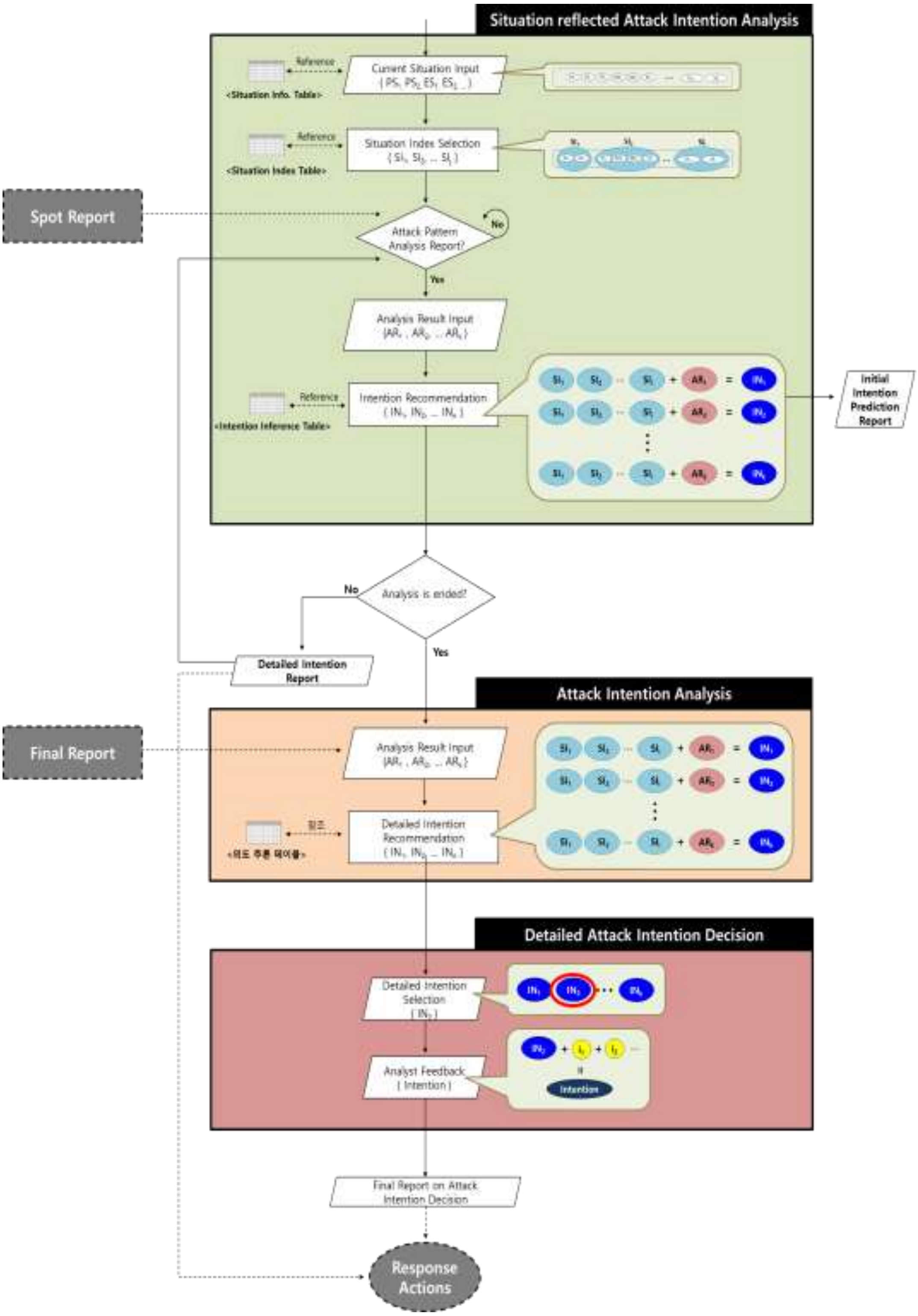
Situation reflected Attack Intention Analysis
Reference
<Situation Info. Table>
Current Situation Input
{ PS, PS, ES, ES, ... }
Reference
<Situation Index Table>
Situation Index Selection
{ SI, SI, ... SI }
Spot Report
Attack Pattern
Analysis Report?
No
Yes
Analysis Result Input
{AR, AR, ... AR}
Reference
<Intention Inference Table>
Intention Recommendation
{ IN, IN, ... IN }
SI SI ... SI + AR = IN
Initial
Intention
Prediction
Report
No
Analysis is ended?
Yes
Detailed Intention
Report
Attack Intention Analysis
Final Report
Analysis Result Input
{AR, AR, ... AR}
참조
<의도 추론 테이블>
Detailed Intention
Recommendation
{ IN, IN, ... IN }
Detailed Attack Intention Decision
Detailed Intention
Selection
{ IN }
IN IN ... IN
Analyst Feedback
{ Intention }
IN + I + I ...
=
Intention
Final Report on Attack
Intention Decision
Response
Actions

Figure 3. The Situation Reflected Attack Intention Analysis Module

The second step is the process of extracting the situation index, which is converted into the situation index by referring to the situation index(SI) table like the following table. In the situation index table, a list of the situation index constituting each index is stored. In the situation index table, a list of the conditions constituting each index is stored. An index is extracted that accurately matches the collected information with the situation list of the table. Based on the case of cyber-attacks over the past decade, the situation index has extracted, and cataloged political, economic, social, and military affairs related to cyber- attacks or both domestic and international hot issues at the time of cyber- attacks.

Table 10. An Example of the Situation Index Table

ID Number	Contents	Situation List
SI0001	Increase in internal crisis in nation A	PS0025, SS0014
SI0002	Increase in internal crisis in nation A	SS0011, SS0002, SS0001
SI0003	External provocation of nation A	MS0001, SS0015
SI0004	External provocation of nation A	MS0002, SS0015
SI0005	Resistance to nation A’s sanctions	PS0005, SS0016
…	…	…

The third process reflects the report of the attack analysis, which is simply inputting attack result data from the attack analysis result in spot report.

The fourth process is an intention recommendation process, which is a process of determining what intentions can be seen when fusing previously transformed situation index and attack result data. The above information is stored in the intention reasoning table, and it is sufficient to find a record in which each converted situation index and attack result data are exactly matched. The intention reasoning table refers to the detailed intention Table(IN) like Table 11. The detailed intention table is an analysis of cyber- attack cases over the past decade to extract the attacker's intentions. When the intention recommendation process is completed, the initial intention prediction report proceeds. In this time, meaningful intent analysis results may appear, but since intention analysis is performed only with the first attack indication information, it will be focused on reporting the attack progress pattern and current situation.

Table 11. An Example of the Detailed Intention Table

ID Number	Detailed Intention
IN0001	Ability ostentation
IN0002	Monetary benefit
IN0003	Manipulation of opinion
IN0004	Propagation and agitation
IN0005	Disorder of social order
…	…

When the attack pattern analysis process is completed, the process of the situation reflected intention analysis is ended and the process of attack intention analysis determination is proceeded. At this time, the detailed intention is recommended by fusing the existing situation index and the final attack pattern analysis results. The detailed intention extraction uses an intention reasoning table(IR) like the following table, which includes an attack result list, a situation list, and an intention list.

Table 12. An Example of Intention Reasoning Table

ID Number	Intention List	Situation List	Attack Results List
IR0001	IN0017, IN0018	SI0001	AR13, AR12, AR01
IR0002	IN0001, IN0018	SI0023	AR13, AR12, AR01
IR0003	IN0020, IN0033, IN0034	SI0053	AR13, AR21
IR0004	IN0024	SI0063, SI0066	AR13, AR12, AR02
IR0005	IN0013, IN0014	SI0193, SI0180	AR06
…	…	…	…

When the above process is ended, the detailed attack intention determination process is executed. At this time, the analyst recommends the most reliable detailed intention of the recommended detailed intentions in the previous process based on additional information such as duty know-how and confidential information.

After all the processes are completed, it is reported to the final attack intention determination and provided to the response actions, administrators and related organizations.

5. Conclusion

In this paper, we propose a cyber- attack intention analysis model that can identify attack intentions to achieve through cyber- attacks or quickly determine enemy intentions so that more damage does not occur. The difference from the existing research is that the current situation of domestic and international situation is used as an analysis index for cyber- attack intention analysis. The association analysis shows how much the domestic and international situation affects the cyber-attack or how the cyber- attack affects the domestic and international situation.

Index for the intention analysis were composed of index for the cyber- attack analysis module and index for the situation analysis module. The index related to the cyber- attack analysis were derived from the analysis of the cyber- attack pattern that have been a hot issue during the cyber- attacks in the past 10 years. the attack indications are extracted and classified by the attack subjects, types, techniques, and results. The analysis of the situation analysis lists important domestic and international situations before and after the cyber- attack in terms of political, economic, social and military aspects.

In future, it is expected that the reliability of the data extraction and the accuracy of the intention analysis will be increased and the analysis time will be shortened if the automated program is developed using the proposed cyber- attack intention analysis model.

Acknowledgements

"This paper is a revised and expanded version of a paper entitled [Architecture of Cyber Intelligence System for Cyber- attack & Defense Training] presented at [ITCS 2016, Indonesia and 5~8 July]."

References

[1] J. H. Eom, "A Study on the Development and Determination of Intention Analysis Index of Cyber-attack", Daejeon University Publishers, Daejeon, **(2017)**.

[2] H.Y. Jung, "Strategy of coercion through cyber- attack", Journal of the Korean association of international studies, **(2016)**, pp. 1-16.

[3] S.-M. Park and J.-I. Lim, "Study on Identifying Cyber- attack Classification Through The Analysis of Cyber- attack Intention", Journal of the Korea Institute of Information Security & Cryptology, vol.27 no.1**, (2017)**, pp.103-113.

[4] W. Kim, C. Park, S. Lee and J. Lim, "Methods for Classification and Attack Prediction of Attack Groups based on Framework of Cyber Defense Operations", Journal of KIISE : Computing Practices and Letters, vol.20 no.6, **(2014)**, pp.317-328.

[5] D. I. Jin Chun and H.C. Eun, "Association Rule Mining on Viewing Rate Analysis: In Case of Drama Genre of Terrestrial Broadcasters", Korean Journal of Journalism & Communication Studies, vol.58, no.5, **(2014)**, pp.391-416.

[6] https://namu.wiki, 17 July **(2017).**

[7] X. Qin and W. Lee, "Attack Plan Recognition and Prediction Using Causal Networks, the 20th Annual Computer Security Applications Conference", Arizona, USA, **(2004)**, pp.1-10.