Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System

Minhee Joo
Institute of Cyber Security & Privacy (ICSP)
Korea University
Seoul, Republic of Korea
Email: mhjoo9321@korea.ac.kr

Junwoo Seo
Department of Cyber Defense (CYDF)
Korea University
Seoul, Republic of Korea
Email: junuseo@korea.ac.kr

Junhyoung Oh
Institute of Cyber Security &Privacy (ICSP)
Korea University
Seoul, Republic of Korea
Email: ohjun02@korea.ac.kr

Mookyu Park
Institute of Cyber Security &Privacy (ICSP)
Korea University
Seoul, Republic of Korea
Email: ctupmk@korea.ac.kr

Kyungho Lee
Institute of Cyber Security &Privacy (ICSP)
Korea University
Seoul, Republic of Korea
Email: kevinlee@korea.ac.kr

***Abstract*—Recently, IoT, 5G mobile, big data, and artificial intelligence are increasingly used in the real world. These technologies are based on convergenced in Cyber Physical System(CPS). CPS technology requires core technologies to ensure reliability, real-time, safety, autonomy, and security. CPS is the system that can connect between cyberspace and physical space. Cyberspace attacks are confused in the real world and have a lot of damage. The personal information that dealing in CPS has high confidentiality, so the policies and technique will needed to protect the attack in advance. If there is an attack on the CPS, not only personal information but also national confidential data can be leaked. In order to prevent this, the risk is measured using the Factor Analysis of Information Risk (FAIR) Model, which can measure risk by element for situational awareness in CPS environment. To reduce risk by preventing attacks in CPS, this paper measures risk after using the concept of Crime Prevention Through Environmental Design(CPTED).**

***Index Terms*—IoT, CPTED, FAIR Model, Risk Management, Situational Awareness, Cyber Physical System**

I. Introduction

With the advancement of the Internet of Things (IoT) technology, we have been able to quickly, accurately and precisely collect the desired data in the real world. Jayavardhana Gubbi studied the vision and future direction in Internet of Things(IoT) environment where internet and things are converged [1]. Cyber Physical System(CPS) is the connection between cyber space and real world. Like the IoT environment CPS collects and analyzes data from a variety of complex worlds, and then feedback the results to the real world. CPS will provide more reliable and realistic information to interact with the real world. CPS providing innovative services in various fields such as traffic, medical power, etc., and bring about a big change in the real world. CPS is a system that deals with a lot of national confidential information such as defense, aerospace, automobile, chemical, urban infrastructure, energy, etc.

Yongsoon Eun pointed out that security in CPS is one of the fundamental problems to be solved for activation of smart grid [2]. Attacks that using CPS and real-world feedbacks have a negative impact on information or services that use the CPS environment. In cyberspace there are many crimes. A typical example is Ransomware, such as Wannacry, whose purpose is to steal money. If CPS attacked by cyber attack like Ransomware, it can cause social turmoil. This paper attempts to reduce the risk of cyber attacks in CPS environments.

In order to reduce the risk, use the prevention design model Crime Prevention Through Environmental Design (CPTED), which has already been proven as a crime prevention environment model in architecture, urban designs and various fields. In the early 1990s, serious social problems such as violence, robbery, property damage, and drug dealing were raised at Dayton, Ohio, United States of America. To solve these serious problems Newman's 'Defensible Space Theory' was used in Dayton City. Defensible Space Theory is the only physical element of urban space that is related to crime [3]. This theory is the background of CPTEDs main two factors. The two factor is surveillance and territoriality. In order to prevent crime, Dayton city carried out regulations on building type and size, regulation of land size, designation of construction line and regulation of building materials. As a result, five years after the end of the project, the crime rate in Dayton city decreased by 25%. Housing theft, robbery, and car theft rate were the lowest in five years. In this paper, we measure the risk of cyber attacks at cyber level among CPS environments and compare

the risk after applying CPTED.

II. Background

This paper measures the risk in CPS. This section describes the CPS environment and describes the FAIR model that can measure risk. Moreover, the paper proposes CPTED as countermeasure method to reduce the risk and explain cyber situational awareness to make effective decision making in CPS environment.

A. Cyber Physical System(CPS)

CPS is a dependable system that controls real systems or processes as a result of physical environment information processing on cyberspace. CPS technology can be extended to various convergence IT fields based on the development of computer, communication and control technology, and can be applied to various fields(e.g. automatic pilot avionics, autonomous automobile systems, process control systems, robotics systems and medical monitoring) requiring high reliability such as aviation, defense, manufacturing, transportation, medical . Jay Lee et al. said that in the early development stage of Industry 4.0, a clear definition of CPS is needed and proposed integrated five-level architecture as a guideline for implementing CPS [4].

1) Connection (Smart connection): The first step in developing a CPS is to get accurate and reliable data from the computer and its components. Two important factors should be considered at this level. First, in situations where certain protocols such as MTConnect are useful, it is necessary to manage data collection procedure data collection procedures in a smooth, tether-free manner, taking into account the various types of data and transferring the data to a central server. The second is to select the appropriate sensor.

2) Conversion (Data-to-information conversion): Meaningful information must be deduced from the data. To improve the level of data-to-information conversion, use tools such as the Decision Support System (DSS). By prioritizing and optimizing decision, the second level of CPS architecture is to provide the machine with self-awareness.

3) Cyber: The cyber level serves as the central information hub of the architecture. A system network is formed by sending information from all connected machines. When a huge amount of information is collected, a specific analysis should be used to extract additional information that provides better insight into the condition of the individual machines. This analysis provides the system with its own comparison function that can compare and evaluate the performance of a single machine with a vehicle. On the other hand, similarities between machine performance and historical assets can be measure to predict the future behavior of the machine.

4) Cognition: At this level, a thorough knowledge of the monitored system can be gained. The user can make a decision based on the analysis information provided. At this level, appropriate information graphics are needed to fully transfer the acquired knowledge to the user.

5) Configuration: The Configuration level provides feedback from cyberspace to physical space. This level also configures the machine itself and performs supervisory control so that it can adapt itself. Finally, this level acts as a Resilience Control System (RCS) that applies decisions made at the perceptual level to the system.

B. Cyber Situational Awareness(CSA)

Cyber Situational Awareness (CSA) is the recognition of the environmental elements of time and space that occur in cyber space that guarantees anonymity. CSA is based on Endsley's model. In 1995, Endsley's model consists of the perception or detection of the environment, the perception of the environment, and the process of predicting the future environment [5].

The CSA is divided into three levels. Perception of information, Comprehension of current situation, and Projection of future status. Perception of information is the most basic level of information and clues in the environment. This means analyzing the dependency between threat and asset and mission. Comprehension of the current situation is a step that can recognize the current situation based on the collected information in perception of information level. In this level the meaningful information can provide. Projection of future status is to recognize the information, understand it as the current situation, and project it on the future environment based on the information or circumstances. This cyber situational awareness establishes a safe cyber environment by decision making by perception, comprehension, and projection.

C. FAIR(Factor Analysis of Information Risk) Model

This study applied FAIR model to measure the risk of crime in CPS environment. The FAIR model is a model that measures risk through factors that can affect risk. FAIR Methodology was first proposed by Jack A. Jones and a detailed methodology is introduced in his journal [6]. This study conducted FAIR analysis through the methodology and terminology presented in his journal. The FAIR methodology classifies each factor into five levels from Very Low to Very High. Moreover, FAIR model classifies risk through the Loss Event Frequency (LEF), the frequency at which threats occur, and the Loss Magnitude (LM) when threatened. The FAIR model is categorized by the classification of factors contributing to risk and the way they affect each other. It can be used as a practical decision-making tool in the cyber space based on the scenario-based analysis of the possibility of a threat and quantitative measurement.

The threat information element of the FAIR model obtains the Loss event frequency(LEF), due to the weakness of system and the enemy threat frequency. Another factor to the threat is the loss magnitude (LM) according to the threat. It is a model to judge the final threat based on the loss event frequency and loss magnitude according to the threat. Contact Frequency (CF) and Probability of Action (PoA) yield the Threat Event Frequency (TEF). Threat Capability (Tcap) and Control Strength yield the Vulnerability (Vuln). The primary

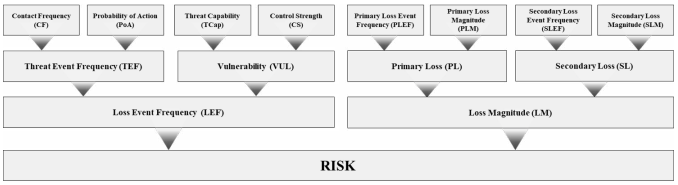

Fig. 1. Measure risk by factors

loss magnitude (PLM) and the primary loss event frequency (PLEF), which measures the delay time, are used to calculated the primary loss. Secondary loss magnitude (SLM) and the secondary loss event frequency (SLEF), which measure recovery usability, are then used to calculated the secondary damage caused by the threat. This can be represented as a fig.1.

Additionally, in order to set the LEF in the FAIR model, profiling of the threat agent is required. These profiling elements are called Threat Community (TCom). The profiling component of TCom consists of motive, primary intent, sponsorship, preferred general target characteristics, preferred targets, capability, personal risk tolerance, and concern for collateral damage.

FAIR measures the risk through the combined result of each factor. In this study, the psychological risk of human beings due to Ransomware attacks can be measured because the loss of assets can be measured by not only the primary loss for the cyber threat but also the secondary loss.

D. Crime Prevention Through Environmental Design(CPTED)

CPTED is a environmental design that reduces the crime and anxiety by planning and changing the environment. This design is to eliminate or minimize the crime opportunity in the urban and architectural space through modifying and designing surrounding space. In the United States, the United Kingdom, Australia, the Netherlands, and Japan, the history of related fields has been long, and it has been widely used in cities, architecture. Nowadays a lot of nations research in IoT field to prevent crime. CPTED process has six levels, but some field consider two or three kinds of factors. The principle of CPTED focuses on access control and monitoring [7]. The application principles of CPTED are surveillance, access control, territoriality, activity support, management maintenance, legibility.

1) Surveillance: Surveillance at CPTED is a principle that enhances crime monitoring. To enhance surveillance are divided into natural surveillance and mechanical surveillance. Natural surveillance induces the behavior of potential criminals and victims to be in the line of sight through spatial arrangement and facility design. Mechanical surveillance mainly uses CCTV for security. If CCTV is installed, the crime rate will not fully disappear, but it will decrease.

2) Access Control: In order to access control of criminal there are two methods. Two method is change the spatial design or facility design. Spatial design creates an environment that guides people's behavior in a certain pattern. Facility design is to remove hide space or to prevent attempts to enter buildings in unusual ways.

3) Territoriality: Territoriality has direct or indirect control over antisocial behavior in a clearly defined area through spatial layout and facility design. Therefore, it increases the psychological burden of criminals and increases the likelihood that criminal activity will be detected cite brown1993residential. Thereby reinforcing the sense of responsibility and compliance with the surrounding environment.

4) Activity Support: Activity support is a design that leads to various activities linked to nature monitoring. By designing the environment to actively use people's spaces and facilities, they naturally increase the opportunities for surveillance and crush criminal behavior.

5) Management & Maintenance: Management Maintenance is related to Access Control and Territoriality. Use facilities that can maintain the crime prevention function steadily. In a declining or unmanaged environment in the Broken window Theory, it can happen from a minor misdemeanor to a serious violent crime [8]. In architecture, it is important to keep the environment as it was originally designed, based on the people's interests and responsibilities.

6) Legibility: Legibility is designed to make spatial and facilities easy to recognize and use properly. In general, it is effective to reduce the anxiety of crime in the area where clarity is emphasized and the behavior of criminals may passively shrink. Design an information that about facilities and the method that using facilities disposed at visible and easy to understand, then it can prevent opportunities to enter so the risk of crime will decline in advance.

III. Related Works

The risk analysis for CPS has been done in various aspects. C. Warren Axelrod emphasized that the overall risk of the CPS is greater than the sum of the risk of the component system [9]. To assess and mitigate this overall risk, it was necessary to understand the threats to the data processing system and the risks that could arise in software that controls the physical system. Finally, he enumerates the overall risk and suggests how these elements can be reduced or eliminated in systems where safety is important. Stamatis Karnouskos investigated how Stuxnet worm, a highly sophisticated attack, affects CPS [10]. As a result, they have successfully proved the validity of the Stuxnet attack and said it is absolutely necessary to invest in security by looking at the system as a whole when designing the CPS. However, these papers lack structured analysis and improvement frameworks. The paper therefore present a new framework for analyzing and improving the risk of CPS by fusing existing structured frameworks.

There have been many researches that six major principles that consists CPTED which reduce crime. Kate Painter has done research that reduces the amount of crime by installing lights on the streets cite painter1999improved. It is said that if street lighting and CCTV is installed, crime can be reduced. But the most important thing is to recognize the present situation well. Carrie Casteel explained that the CPTED approach

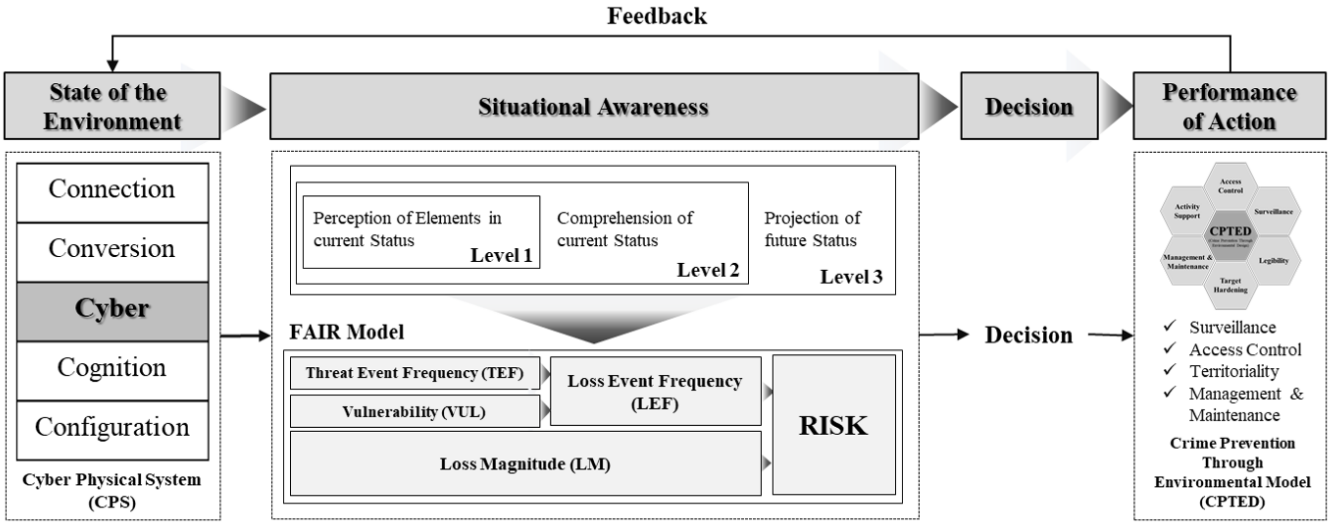

Fig. 2. Step of Situational Awareness Framework for Cyber Crime Prevention Model in Cyber Physical System

can be adapted to all settings and results by considering the six principles of CPTED (surveillance, access control, territoriality, activity support, management maintenance, legibility) [11]. Also CPTED is an effective approach to reduce the intensity of crime prevention. There is still a lack of research on the effects on CPTED. Also the research that integrate the CPTED and other fields are less. In this paper, we combine CPTED generated in cyberspace to measure the risk of attack and reduce the risk.

IV. Proposal Method

Prior to improving the CPS, situational awareness of the current CPS should be prioritized. For the current CPS context, this paper selected Endsley's Model. Endsley's model consists of four phases: State of the Environment, Situational Awareness, Decision, and Performance of Action. After the Performance of Action phase, flow goes back to the State of the Environment, which is the first phase. This paper introduces the FAIR Methodology to systematically perform the Situational Awareness step of Endsley's Model. FAIR Methodology is used to quantitatively calculate the risk of the current CPS. The decision is made through a quantitative calculation of the risk value, and the decision maker presents a countermeasure against the CPS with a high risk value. This paper presents CPTED as a countermeasure. In the Performance of Action phase, CPTED is applied to the CPS, which is feedback to the first stage.

CPTED consists of six principles: surveillance, access control, territoriality, activity support, management & maintenance, and legibility. This paper focuses on 4 principles among 6 principles. First, this paper introduces a surveillance principle in the cyber layer of CPS. With continuous surveillance, a system accumulates threat data to measure the weight of the each threat. Next, reinforce the territoriality of the cyber layer. By strengthening territoriality, the attacker's probability of action (PoA) on the cyber layer can be lowered. If these two elements are preventative principles, then the next principle is a direct defense principle. It updates data of attacker in the past in real time, classifies the attacker's characteristics and measures the weight, and performs direct access control of the method of blocking attack over a certain weight. This is the factor that lowers the contact frequency (CF), which can be combined with the preceding principle, resulting in a lowering of the threat event frequency (TEF). Finally, the management & maintenance principle manages factors that continuously impact the risk. The overall flow chart of this paper is shown in Fig.2.

V. Result

A. State of the Cyber Physical System(CPS)

The relationship between the physical system and the control software has been developed to simplify and systematize from the design stage to predict reliability. Cyber Physical System (CPS), which is being developed, is now increasingly used by combining manufacturing and IT. It connects manufacturing and IT stores information such as a smart increase plant productivity implementation.The company using CPS stored a lot of confidential information. In the case of a company using a CPS that stores a lot of confidential information of the company, the CPS may be damaged in delivery as well as manufacturing in case of an attack. In this paper, the environmental perception of CPS is used to measure risk as an FAIR model. To reduce the risk by adjusting the countermeasure using CPTED, and can compare the risk before and after.

B. Situational Awareness in Cyber Level using FAIR Model

In this paper, the research was conducted based on data of cyber threat recorded in A-company in 2013 [12]. In March 2013, there was a honeypot attack on A-company. The

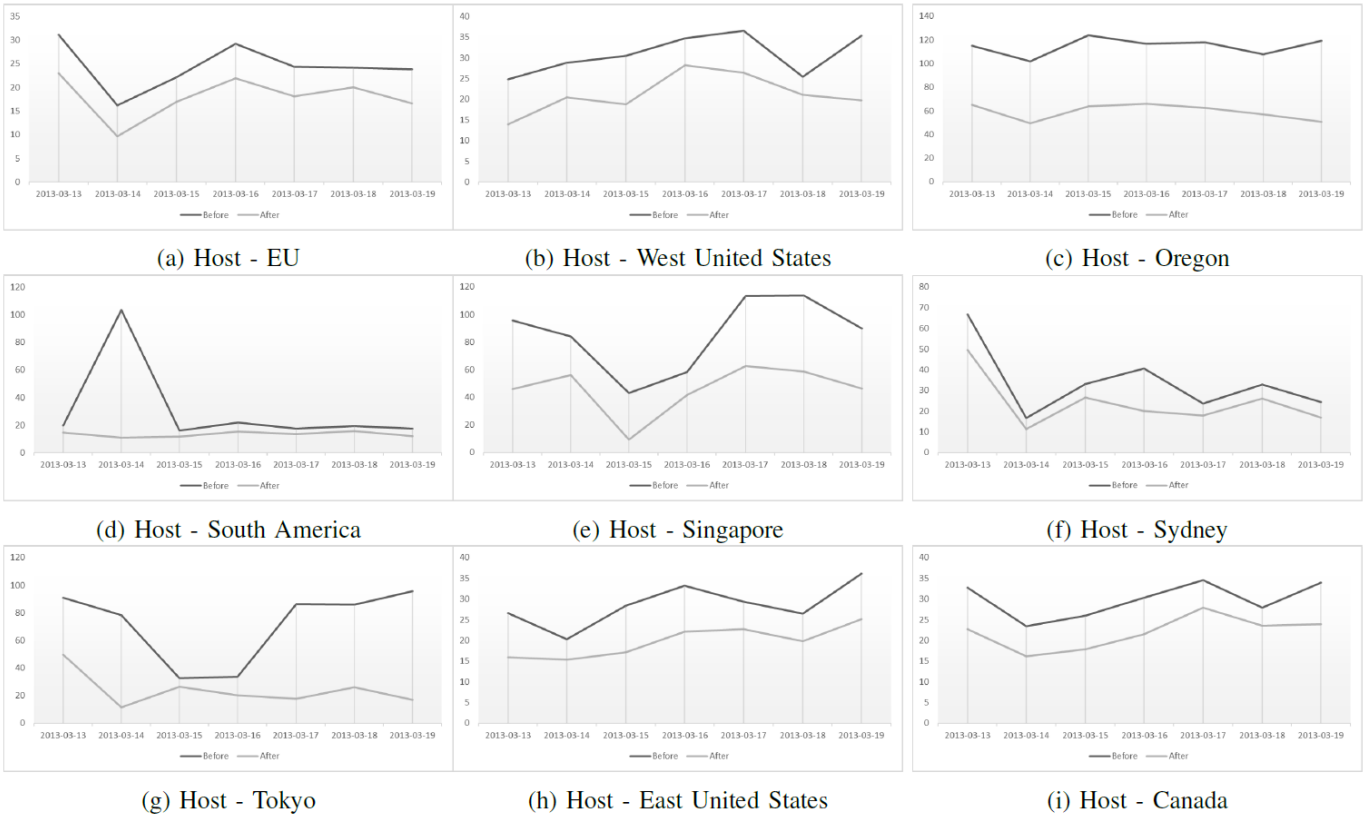

Fig. 3. Risk of Each Host (Before: Black Line / After: Gray Line)

risk is measured taking into account the frequency of the Honeypot attack and the size of the loss of the A-company when attacked. From March 13, 2013 to March 20, 2013, the paper investigated the weekly attacks by server. To calculate this risk, frequency and magnitude are needed. For frequency, the Loss Event Frequency (LEF) is calculated as Threat Event Frequency (TEF) and Vulnerability (VUL). Magnitude is calculated by Loss Magnitude (LM). In this paper, the risk is measured using TEF, VUL, and LM. The TEF was limited to the nine countries that had the most attacks in a week. The paper limited VUL to IP protocol, which is the most vulnerable to spoofing attacks. In the IP protocol attack, the highest risk is 79.4% for TCP, 15.9% for UDP and 4.5% for ICMP [13]. Depending on the type of attack, the value could be calculated. TEF and VUL are completely independent. The LEF was calculated using Joint Probability to measure the probability of two independent risks. LM represents the magnitude of the loss, which is material that is not disclosed by the company. Therefore, this paper estimates the number of customers per server based on the service price of EC2 type of A-company. It is assumed that the number of customers is larger as the value is closer from the average per server, and that the number of customers is smaller as the value is farther from the average. Risk was also measured using Joint Probability. The server-specific risk values are shown in black lines in the fig.3.

C. Risk Decision

According to the framework proposed in the paper, based on the measured risk values, the third step of Endsley's Model is the Decision step. Decision makers must take action to reduce risk to stabilize CPS. This paper attempts to introduce CPTED into CPS to reduce the risk of CPS. In other words, CPTED is selected as a countermeasure to reduce risk in the performance of action, the fourth stage of Endsley's Model. After introducing CPTED in CPS, feedback process is performed to verify the effect of countermeasure.

D. Performance of Action using CPTED

Next, this paper measures the risk in the CPS environment designed as proposed in the proposal method. In the same way as the data before the introduction of CPTED, the risk is calculated in the same way, and the risk value for each server is indicated by the gray line of the figure. As a result, it can be seen that the introduction of CPTED reduced the risk by an average of 30%. Prior to applying CPTED, all threats were high. Host-EU, West United States, Oregon, South America, Singapore, Sydney, Tokyo, East United States, Canada. Overall, the risk of all hosts is lowered. South America was significantly lower. The reason is that the countries that are constantly attacking are only one, giving weight only to that country, and it is lowered. It can be seen that by adjusting only the frequency of frequent attacks, the risk is reduced

by almost two times. Fig.3-(d) shows the result. Host-Sydney remains the same before and after the risk. But the risk has decreased. Thus, all hosts from Fig.3-(a) (i) show that the risk is reduced when CPTED is applied.

VI. Conclusion

Ubiquitous networking and IoT, the physical world where everything is connected, has already become part of our lives. The security of the CPS that connects everything such as services or data is as important. Decisions and judgments in the CPS are based on the collected data. These data should be prepared for the risks and uncertainties that are associated with privacy and security. CPS aims at autonomy without human intervention but eventually it is human-centered system, and the security of data about human is weak when CPS is attacked.

Therefore, in this paper, we use Endsley's Model for situational awareness of CPS. Risk was calculated using the FAIR model used to measure risk at the Situational Awareness. The risk was reduced by applying CPTED to the measured high risk in the FAIR model. By applying real attack data, it is possible to lower the value of risk and defend against attacks in CPS.

Furthermore, companies that use CPS can apply CPTED's platform to cyberspace, reducing the risk of CPS attack. And also by using Machine Learning and Deep Learning in CPS, you can continue to learn the past data to prevent attacks on all areas using CPS.

VII. Acknowledgments

This research was supported by the MSIT(Ministry of Science, ICT),Korea, under the ITRC(Information Technology Research Center) support program (IITP-2018-2015-0-00403)supervised by the IITP(Institute for Information & communications Technology Promotion)

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[2] Y. Eun, K. Park, M. Won, T. Park, and S. Son, "Recent trends in cyber physical systems research," *Communications of the Korean Institute of Information Scientists and Engineers*, vol. 31, no. 12, pp. 8–15, 2013. [Online]. Available: http://www.dbpia.co.kr/Article/NODE02330861

[3] O. Newman, *Creating defensible space*. Diane Publishing, 1997.

[4] J. Lee, B. Bagheri, and H.-A. Kao, "A cyber-physical systems architecture for industry 4.0-based manufacturing systems," *Manufacturing Letters*, vol. 3, pp. 18–23, 2015.

[5] M. R. Endsley, "Toward a theory of situation awareness in dynamic systems," *Human factors*, vol. 37, no. 1, pp. 32–64, 1995.

[6] J. Jones, "An introduction to factor analysis of information risk (fair)," *Norwich Journal of Information Assurance*, vol. 2, no. 1, p. 67, 2006.

[7] D. Kim and S. Park, "Improving community street lighting using cpted: A case study of three communities in korea," *Sustainable cities and society*, vol. 28, pp. 233–241, 2017.

[8] G. L. Kelling and C. M. Coles, *Fixing broken windows: Restoring order and reducing crime in our communities*. Simon and Schuster, 1997.

[9] C. W. Axelrod, "Managing the risks of cyber-physical systems," in *Systems, Applications and Technology Conference (LISAT), 2013 IEEE Long Island*. IEEE, 2013, pp. 1–6.

[10] S. Karnouskos, "Stuxnet worm impact on industrial cyber-physical system security," in *IECON 2011-37th Annual Conference on IEEE Industrial Electronics Society*. IEEE, 2011, pp. 4490–4494.

[11] C. Casteel and C. Peek-Asa, "Effectiveness of crime prevention through environmental design (cpted) in reducing robberies," *American Journal of Preventive Medicine*, vol. 18, no. 4, pp. 99–115, 2000.

[12] "Aws honeypots marx geo," 2013. [Online]. Available: http://datadrivensecurity.info/blog/data/2014/01/marx-geo.tar.gz

[13] M. Jonker, A. King, J. Krupp, C. Rossow, A. Sperotto, and A. Dainotti, "Millions of targets under attack: a macroscopic characterization of the dos ecosystem," in *Proceedings of the 2017 Internet Measurement Conference*. ACM, 2017, pp. 100–113.