Review Article

International Journal of Advanced Computer Research, Vol 9(40)
ISSN (Print): 2249-7277 ISSN (Online): 2277-7970
http://dx.doi.org/10.19101/IJACR.SOC6

A leading cyber warfare strategy according to the evolution of cyber technology after the fourth industrial revolution

Sin-Kon Kim[1], Sang-Pil Cheon[2], and Jung-Ho Eom[3*]
Maintenance Officer (Colonel), RoK Airforce, National Defense University, Seoul, Korea[1]
Professor, Military Studies at Daejeon University, Daejeon, Korea[2]
Associate Professor, Military Studies, Daejeon University, Daejeon, Korea[3]

Received: 25-May-2018; Revised: 27-July-2018; Accepted: 5-October-2018

Abstract
As science, technology is vertically advanced or horizontally combined with information and communication technology. The boundaries are broken down in all areas of physical, biological space, and cyberspace, connecting all objects in the world. Cyber battlefields are becoming more complex and intelligent in the future, so it is not possible to dominate cyber battlefields with the current cyber warfare strategy and security technology. Future cyber warfare strategy should be conceived considering the change of cyber battlefield environment and the new functions of cyber-attack tools, assuming that new science technology and information & communication technology are applied to cyber battlefield. First, we predict the change of cyber battlefield environment and the evolution of cyber-attack technology, according to the development level of current information & communication technology and we propose a cyber warfare strategy in aspect of strategic, operational, and tactical levels that can prevent future advanced cyber threats.

Keywords
Cyber warfare, Cyber strategy, First and depth strategy, Concentration and distribution operation, Maneuver tactics.

1.Introduction
In February 2018, the US foreign ministry reported that the United States has made massive preparations for a massive cyber-attack on North Korea over the past six months. Although it is focused on the preemptive strike on the North Korea, which is called the "Kofi Operation" of the United States, the Donald Trump administration's first attack on the North Korean will be a cyber-operation, not a military attack, the media said [1]. The United States is developing from the concept of defensive cyber operations to the concept of offensive cyber operations for effective cyber warfare of cyber command. The other development countries as well as the United States are shifting the concept of cyber operation from defensive concepts to offensive or preemptive attacks. Recently, developed countries have shifted cyber warfare strategy from a defensive strategy to offensive strategy. If innovative science technologies and cutting-edge information & communication technologies (ICT) are applied to cyber battlefield, cyber-assets cannot be effectively protected by defensive operations anymore.

The cyber battlefield will be applied to advance ICT such as mobile network, big data, Internet of Things (IoT), artificial intelligence (AI), drone, and augmented reality, and it will also apply to cyber-attack tools. In the field of military, all military information will be communicated through the network, and most of the warfare infrastructure system will consist of soft resources. In addition, the weapon system will be equipped with software up to a single platform, and will have the most advanced and high precision, and firepower. It can secure the dominance of the cyber battlefield by paralyzing the battlefield grid, acquiring the military information of the opponent country, and controlling the software of the weapon system platform. The leading cyber operation is judged as a more appropriate concept to secure the superiority of the cyber battlefield in the future. So we need preemptive strategy, operations and tactics that are consistent with future cyber battlefield environments.

Cyber battlefield will become more and more difficult to distinguish from physical space, and will be transformed into a hyper-connected, super-

*Author for correspondence

intelligence, and cross-domain. Human-oriented cyber-attack tools will be developed, which it can penetrate more sophisticated and secretly by applying artificial intelligence, deep learning, pattern recognition, and neural network technology to attack algorithms. Therefore, a new concept of cyber warfare strategy is needed to secure superiority in the cyber battlefield as predicting the changes of the cyber battlefield environment and understanding the functions and characteristics of the new cyber-attack tools. The new concept of cyber warfare strategy should be established in strategic, operational and tactical aspects based on the concept of military strategy [2, 3].

In section 2, we describe the advancement of cyber technologies and predict advanced functions of cyber-attack tools in section 3. We propose a leading cyber warfare strategy that can effectively operate against future cyber threats in section 4, and conclude in section 5.

2.The evolution of cyber technologies

Trans-human [4], which can enhance human intellectual ability and physical strength, is no longer a strange word. Trans-human has emerged as a fusion of artificial intelligence, robotics, and nanotechnology. Trans-human technology, which is perceived as a more intelligent and physically superior being than a human being, is increasingly being applied in our lives. In addition, 'AlphaGo' [5], a google computer program formerly called a collection of artificial intelligence and deep learning algorithms, has evolved into an artificial intelligence robot that is used in schools and hospitals. Asimo robot [6] which developed by Honda, Japan, has developed technologies to transmit and control commands using electroencephalography (EEG) communications. EEG communication is a brain-computer interface (BCI) [7], which is a technology that can control a computer by human thought or most effectively communicate human ideas to people and things and exchange them.

Trans-human, artificial intelligence, BCI, AI, and other technologies that lead the fourth industrial revolution are applicable in the military field as well as in daily life. Robot suits or wearable robots used for military purposes are complex technologies that combine trans-human technology and EEG communication to overcome the physical limitations of soldiers and farther and faster move them [8]. Artificial intelligence and deep learning techniques have been applied to unmanned combat systems, allowing them to autonomously navigate, identify enemy movements and detect targets. Recently, the ability of unmanned aerial vehicle, unmanned submarine, and unmanned military robots are judged to be applied level of artificial intelligence technologies such as analytical ability, learning ability, and prediction ability that enable autonomous operation of unmanned systems [9]. The application of this technology to the military field is at an early stage, but after the 4th industrial revolution, it will be resulted in a completely different form of battlefield as more diverse and advanced science technology and information & communication technologies will be applied to the battlefield. The advanced science technology and information & communication technologies that can be applied to the military field are as follows. However, we restricted the technology applied to cyber battlefield and cyber security in this paper.

Firstly, with technology such as IoT, AI, and optical communication, all combat systems will be in hyper-connection. IoT technology enables real-time connections between objects and between humans and objects, allowing data and information to be freely transmitted. In the future, the development of high-level information and communication technology will enable super logical connection, so that the transmission speed of data over optical communication speed will be more than the speed of light, so that the concept of physical distance will disappear. This will create the same concurrency as sharing the same information in real time in the same place. Even in cyberspace, time cannot be fixed due to the speed of data transmission, and past, present, and future can be distinguished based on the point in time when the data are stored. For example, manipulating data by sniffing is an act of changing the time course in cyberspace.

Secondly, human intelligence-oriented technologies such as artificial intelligence, deep learning, pattern recognition, and deep neural network will be applied to cyber security systems that protect the control software of the unmanned infrastructure system and all cyber assets. These technologies enable unmanned combat systems and battlefield management systems to identify battlefield situations, analyze combat patterns, and learn and execute combat actions. It is still controlled by humans or other control systems at the stage of executing the final action. In the future, the development of innovative programs and algorithms will lead to an autonomous smart combat system that collects and analyzes information on its

own, establishes and executes action procedures, and diagnoses and resolve problems in the event of errors. In addition, smart cyber security systems will be developed that detect threats, analyze attack patterns, and perform countermeasures or recover themselves. The intelligent malicious code also will be developed to disable this security system.

Thirdly, cyber physical system (CPS) [10] is a system that can combine physical real world such as robot, industrial machine, automobile, aircraft, military weapon system, and virtual world including web and software in real time. By using the cyber physical system, the system can recognize the physical world directly beyond the limited ability that human beings can perform, analyze the perceived contents, and have autonomy to react and solve problems itself. A cyber physical system is an automated and intelligent system that interact physical entities co-existing with humans with a cyberspace composed of cyber entities such as sensors and embedded systems through communication, computation, and control. Using the cyber physics system, the unmanned combat system can recognize the physical world directly beyond the limited ability that humans can perform, and can analyze the perceived contents and have the autonomy to react and solve problems. And CPS enables the system to quickly and accurately control physical devices by recognizing, analyzing, and calculating the physical world and providing more accurate information to humans. CPS is currently used only in specific fields due to limited technology, but will be used extensively in large-scale national infrastructure control, strategic weapon system control, and battlefield management system operation beyond the scope of human control in the future.

Fourthly, machine-oriented mind technology can be applied to unmanned remote-control combat systems in near battlefields. The core technology, implanting an electronic chip into the brain, is a technology that transfers brain signals to a computer and transmits computer signals to the brain. In other words, the intention of the controller is transmitted to the unmanned remote control combat system through the brain implant, or the battlefield information collected by the unmanned remote control combat system is transmitted to the controller to know the combat situation. The unmanned remote-control combat system will enhance autonomy, including sensors that can collect battlefield information, big data analysis technology to transmit accurate information in a short period of time, and artificial intelligence capable of battlefield situation judgment.

Finally, there is virtual reality (VR) technology, which refers to a specific environment, situation, or technology that is similar to the real world created by artificial technology using computers. There is also augmented reality (AR) technology, which is a computer graphics technique that combines a virtual object or information into a real environment and looks like an object in the original environment [11]. It is not yet possible to express 100% reality due to the lack of realization of the five senses technology, but after the 4th industrial revolution, it will create mixed reality. Mixed reality [12] is a technology that provides a sense of immersion and presence of mixing physical environment of the real world and virtual environment, and corresponds to a continuous section of real environments and virtual environment. Since the future battlefield is carried out by a smart battle system with minimized human intervention, if a mock combat system is created by using augmented reality or mixed reality technology, the combat system which has the function of collecting, analyzing and judging information by itself can be mistaken for malfunction.

The following *Table 1* shows the summary of cyber technologies applied to the future cyber battlefield.

Table 1 The cyber technology applied to the future cyber battlefield

Cyber technology	Explanations
IoT	-All weapon system components connected to the network
Optical comm.	-The transmission speed of data will be faster
AI, Neural network	-An autonomous smart combat system that collects, analyzes, and spreads data on its own
CPS	-Quickly and accurately control physical combat devices by recognizing, analyzing and calculating the physical battlefield
BCI	-The order of the weapon system controller can be transmitted to the unmanned remote combat system without additional system operation by the controller
VR/AR	-Can create a fake combat system that can confuse the enemy's unmanned combat system

3.Advanced functions of cyber-attack tools

In the future, cyber-attack technology will evolve in a totally different direction from the present aspect, and its destructive power is expected to be enormous. At present, it is not easy to predict the level of development of innovative information and communication technologies, the level of function of the system combined with components of cyber battlefield, the level of human oriented programming language, the level of superposition of physical space and cyberspace, the functions and roles of physical systems and the cyber system after the 4th industrial revolution. And a new cyber-attack tool and cyber security system will be developed to meet the new environment in order to secure superiority in the cyber battlefield. In particular, if technologies such as artificial intelligence, big data, deep learning, and neural networks are applied to cyber-attack technology, they will have a breakthrough and intelligent functions [13−16].

Firstly, human-oriented programs such as artificial intelligence and deep learning technology will be applied to autonomous malicious codes that can analyze the cyberspace environment, detect vulnerabilities and perform attack procedures. In the future, it will be a cyber-battlefield environment in which communication, weapon system, human beings shares combat information and operate on their own, based on the cyber physics system, not the battlefield environment controlled by human intervention. Also, in order to maintain the optimized battlefield environment, the components will identify change patterns and information, and change their configurations and functions themselves. Human-oriented malware will have situation-aware technologies, which identify cyber warfare environments and make calculated decisions about the next steps. The autonomous malicious code has the ability to collect and analyze infiltration intelligence, such as the type of device deployed in a network segment, traffic flow, applications used, transaction details, and transaction time of occurrence. It will have an independent ability to adapt to the enemy's cyber environment while selecting the attack technique according to the target platform when the time to stay in the host becomes longer. It will also have the ability to respond appropriately to the type of security system installed in the host.

Secondly, neural network or reverse coding techniques can be applied to provide stealth and transformer functions. Since the future cyber battlefield has super sensitivity and super intelligence characteristics, the cyber battlefield environment can be configured freely in favor of cyber operations. If traditional cyber-attack agent breaks into cyber battlefields that change from time to time, it can be easily detected and trackbacks by security systems. So, when cyber battlefield environments change, the cyber-attack agent can change its configuration or run it as if it were a unit system of opponent cyber components. In the cyberspace based on cross-platform tools, when the cyber-attack agent penetrates, the transformer function collects information for the loaded platform and selects the appropriate payload using the learning function algorithm, and then selects the penetration method for the target, and combines and executes attack method. It also spreads and penetrates various platforms, widening the scope of threats and making it difficult to detect and trackback. This function injects code and collects data if a vulnerable target is identified, then exploits the vulnerability to remain undetected.

Thirdly, it will also be included self-evolving and mutating functions that incorporate techniques such as pattern recognition and deep learning. Before deploying cyber operations, the cyber ISR (Intelligence, Surveillance and Reconnaissance) agent collects information about the target systems over a long period of time. At this time, when the opponent cyber component is upgraded or changed, the cyber ISR agent is also mutated. Also, if the cyber environment of the opponent changes during a cyber-attack, the cyber-attack agent can change it by predicting change or upgrade through automated big data analysis. In the field of security technology, intelligent detection and prediction based on machine learning and active self-defense techniques are actively being studied. Especially, it is the most advanced security technology equipped with a security algorithm such as machine learning based intruder information and infiltration resource collection, risk prediction technology through correlation analysis, self-learning cyber immunity technology that automatically analyzes and heals software security vulnerabilities. Penetration agent also uses machine learning and deep learning technology to predict target information, change of network and system resource, collects internal network environment information so that security system recognizes it as internal network, and it can self-mutate like internal network component.

Finally, it will be utilized all information assets that make up cyberspace for cyber security. Currently, cyber security is mainly performed in the network, but cyber-attacks and defenses are made using all the means such as sounds, frequencies, electric waves, signals, and brain waves in the between objects and between humans. A cyber security research team at the Gen Gurion University in Israel has developed a new hacking technique that can steal data from computers that are not connected to the Internet by manipulating electromagnetic waves generated from USB. A malicious code called USBee [17], which can control the minute electromagnetic waves generated by USB, is embedded in the USB, and the system is infected when the USB is inserted into the computer. The two frequencies that USB emits, namely the 0 and 1 electromagnetic waves, which are the basis of the digital signal, attacker can obtain data by recognizing the frequency change of the electromagnetic wave by using the wireless antenna in the near. In the past, hacking techniques have been introduced that steal data from computers that are not connected to the Internet by manipulating sound from a computer's cooling fan or resonating sound from a hard disk drive (HDD).

The following *Table 2* shows the summary of the predicted functions of cyber-attacks applied to new ICT in the near future.

Table 2 The function applied ICT to the cyber-attack tool

ICT	The function applied to cyber-attack tool
AI, Deep learning, Situation-aware, etc.	-Self-learning function to analyze cyber battlefield environment, determine enemy targets, and select attack techniques
Neural network, Deep learning, Big data, etc.	-The attack agent has the function to find a new attacking technique by changing itself as a unit element constituting the cyber environment of the enemy, when the cyber environment of the enemy
Sound, Frequency, Electric wave, Signal, EEG, etc.	-The function to utilize all ICT that constitute cyberspace for cyber-attack and defense

4.A leading cyber warfare strategy

After the 4th industrial revolution, the cyber warfare strategy should be constructed as a concrete and a substantive strategy that reflects changes in the cyber battlefield environment and evolved cyber-attack technology. In the cyber battlefield of the future, the concept of time, space, and object will not be an important factor in cyber operations. Therefore, it is not possible to secure the battlefield superiority with traditional defensive cyber warfare strategy or cyber operations. We propose a leading cyber warfare strategy in terms of strategic, operational and tactical aspects considering the change of cyber battlefield environment and the function of cyber-attack technology [14].

The ultimate goal of the cyber warfare is to suppress cyber provocations through a leading cyber operation. In order to secure superiority in a hyper connected and super intelligent battlefield, a leading cyber warfare takes the initiative in all operations related to cyber ISR, cyber electronic warfare, cyber support operations as well as cyber operations, and obtain freedom from all combat acts using the cyber weapon systems. In order to deter the opponent cyber-provocation and to gain dominance in the cyber-warfare, we must collect information, make decisions, and act before the enemy. It should also be able to perform cyber operations in the center of command control, which is the core node of the opponent. To do so, the following strategy should be applied.

From a strategic point of view, we propose an aggressive preemption and in-depth strategy. Firstly, it is necessary to establish a preemptive strategy based on the principles of the 3F (First Watch, First Decision, and First Strike). After the 4th industrial revolution, all combat systems will have the ability to collect information in real time, and software that reflects human thoughts and actions and the information and communication technologies that will not be realized at present will be developed and applied to combat systems. Even science technology that surpasses the concept of classical physics may be introduced and applied. For example, space movement is theoretically possible. The electrons covered by quantum mechanics are particles and have the properties of waves, so they exist stochastically at any time and place in the electronic unit. Such information and communication technologies will be applied cyber operations that should perform surveillance and data transmission faster than opponent on the principle of relativity rather than real-time transmission of data and counter-attack or preemptive defense against attacks. The cyber security process should be faster than opponent

because the cyber battlefield has a hyper-connected, a cross-domain, and super intelligent environment. A hyper-connected network means all objects and humans are connected in real time to each other and are not limited in distance and time to send and receive data or information by IoT, cloud computing and so on. A cross-domain means space where the distinction between physical space and cyber battlefield is broken by CPS. Super intelligent space means that human-oriented software is developed by artificial intelligence technology to do autonomous learning, decision and execution [14]. In order to secure superiority in cyber battlefield, it is necessary to collect information, determine procedures, and conduct actions ahead of opponent in advance. Secondly, it is necessary to build an in-depth defense strategy applying the deep watch, deep control, and deep strike (3D) principles. It should have the ability to monitor and control the opponent's center of gravity to prevent the opponent's cyber-provocation. In other words, it is necessary to identify and continuously monitor the center of gravity where the opponent's core information is stored, and to control to the final core node regardless of which any defense system is built. No matter how much the unit system constituting the cyber battlefield is neutralized, the unit systems can be restored at any time and operated normally. However, if the core command and control system that controls this unit system is disabled, it will not be able to perform its normal function due to information and command transmission error or communication paralysis. Therefore, it is necessary to identify and continuously monitor the opponent command control center, and to deploy cyber operations to the final core node even if any active intelligent defense system is constructed. The following *Figure 1* shows the 3F&3D strategy in terms of strategic cyber operation.

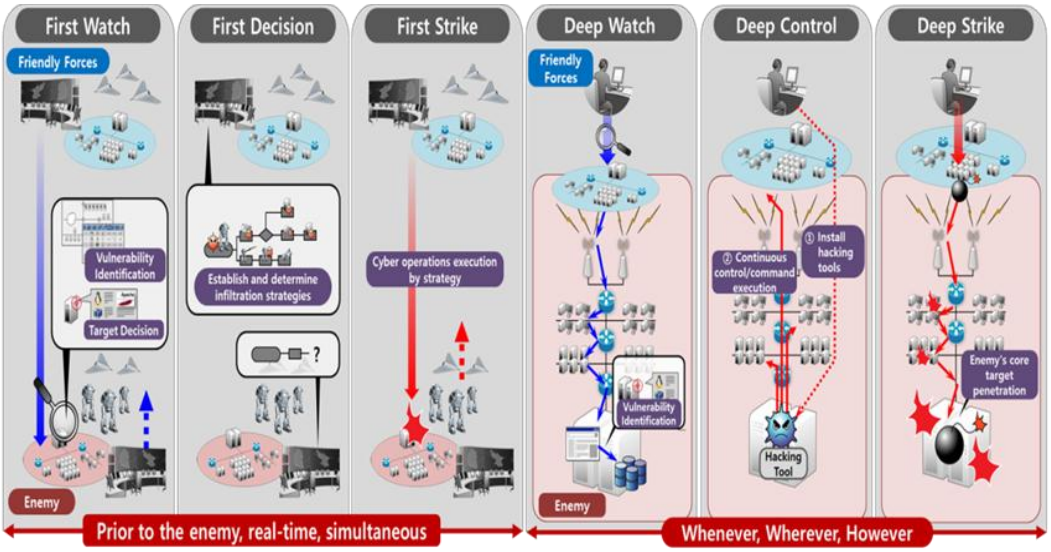

Figure 1 A strategic cyber operation

From an operational point of view, concentration and distribution operations should be deployed. On the offensive side, the concentration and distribution operation are an operation in which all cyber assets are mobilized to concentrate the cyber action on the control system that controls or conducts enemy military operations. Future cyber battlefields will consist of software that allows all things to be connected and self-learning and judgment with minimal human intervention. By installing a cyber-attack agent with these objects, they can penetrate the battlefield and focus cyber behavior on a target. If any objects installed with a cyber-attack agent intentionally insert false information into enemy unmanned combat systems through a snooping attack intensively on a target, the enemy combat system exchange mutual misinformation without authentication of information. On the defensive side, if indications (signs) of an opponent's cyber-attack is detected, all the cyber security systems actively analyze the indications (signs) of cyber-attack, preemptively predict the attack route and pattern, and prevents from infiltrating into the critical system. To prevent opponent cyber-attacks, a central defense control system with cyber-physical system technology is used. The central defense control

system should be able to predict future actions based on data received from all entities, specify the cyber assets required for defense, transmit action policies to be implemented, and control all cyber countermeasures. All cyber assets include artificial intelligence, which collects information about the attack and sends it to the central defense control system. For unit attacks requiring emergency defense, quick action must be taken using self-learning and judgment functions. The following *Figure 2* shows examples of operational cyber operation.

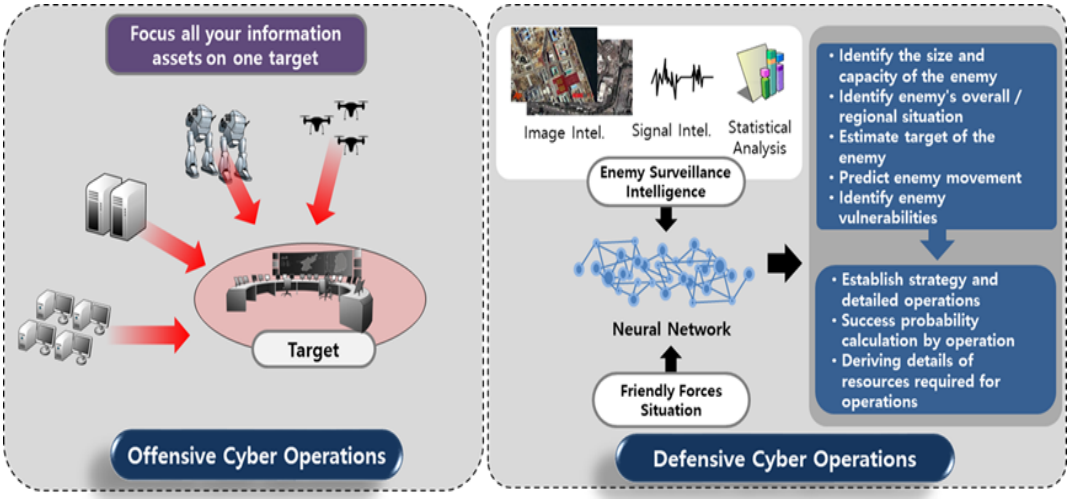

Figure 2 An operational cyber operation

From a tactical point of view, a cyber-battlefield environment-based trigger maneuver (EbTM) tactics should be executed. On the military side, tactics [18] fight and defeat the enemy by using shooting and maneuver as their primary means. That is, it is involved in the kill step in the kill chain process: detection, identification, tracking, targeting, engaging, and evaluation. The cyber kill chain process consists of reconnaissance, weaponization, dissemination, exploitation, installation, command and control, and goal attainment stages. Tactics (maneuver) corresponds from the dissemination to the command and control stage. However, in the future cyber warfare, it is expected that function based cyber action will be deployed rather than sequential cyber behavior due to change of cyber battlefield environment and cyber-attack technology evolution. Cyber maneuver [19] is the process of executing a security program in order to achieve cyber security objectives, so that the security system can block opponent's cyber penetration in advance and trace back and destroy the opponent's attack source. The purpose of a cyber-battlefield environment-based trigger maneuver tactics is to find out and block the source of opponent's cyber-attacks as soon as a cyber-attack is occurred. When a cyber response agent enters the opponent's cyber battlefield to find the opponent's source of cyber-attack, it may often not match the environmental information collected earlier due to the intelligent active defense system, transformer platform, and real-time self-upgrade software, etc. At this time, the cyber response agent changes itself according to the current cyber battlefield environment and changes the tactics of the new attack path and target. This is because a cyber response agent has many human-oriented algorithms, including artificial intelligence, deep neural network, etc. For example, assume that the task of the cyber-agent attack is to gain the privileges of the operating system and that the technique installed before triggering exploits a vulnerability that could grant write access to the Linux kernel 'read-only' domain memory. However, when a cyber-attack agent breaks into the system and identifies to exploit root privilege by exploiting the vulnerability, if the vulnerability has already been patched, the cyber-attack will end in failure. However, if the cyber-attack agent has a human-oriented algorithm, it will identify other vulnerabilities and will reassemble or modify the hacking program to use the penetration techniques accordingly. Eventually, it will exploit the root privilege by finding a vulnerability in the Linux kernel's 'perf_swevent_init' function that makes use the wrong datatype. The following figure shows 'EbTM tactics' in terms of tactical cyber operation.

5.Conclusion

After the 4th industrial revolution, since the cyberspace environment and cyber-attack technology can transcend the current level due to the rapid development of science technology and information & communication technology. Therefore, it is impossible to secure superiority in the future cyber warfare with the existing cyber warfare strategy. It is necessary to change the traditional defensive cyber warfare strategy to an offensive cyber warfare strategy, and to implement the cyber warfare strategy, operation and tactics in accordance with the future cyber battlefield environment. In this paper, we proposed cyber security strategies in terms of strategies, operations and tactics as a leading cyber warfare strategy.

In the strategic aspect, we proposed an aggressive preemption and in-depth strategy. The aggressive preemption strategy is based on the principle of 3F that, collects information, identifies the target, and determines attack or defense before opponent executes. In-depth strategy applied the 3D principle that identifies the center of gravity where opponent command control is performed and continuously monitors, and cyber operations can be deployed to the core node in the center of gravity. In the operational aspect, we proposed concentration and distribution operations. The concentration operation is an operation to mobilize all the cyber assets to focus cyber action on the systems and control systems that control or perform the opponent's military operations.

A distribution operation is an operation in which cyber assets actively respond to cyber-attack according to each other's role by predicting and detecting attack techniques and routes in advance, when indications of cyber penetration of the enemy are identified. In the tactical aspect, we proposed a cyber-battlefield environment based maneuvering tactics. Proposed cyber maneuvering tactics can respond instantly to cyber-attack patterns and cyber battlefield environments. In the future research, we will apply the proposed cyber warfare strategy to the development of an offensive security mechanism and model. Recently, as cyber-attack defense technology using artificial intelligence has been actively developed, we will design active cyber defense model.

Acknowledgment

This paper is a revised and expanded version of a paper entitled [Offensive Cyber Security Strategy according to the Evolution of Cyber Attack Technology] presented at [IDIW2018, Jeju and 11-12 May]. This research was supported by the Daejeon University fund (2016).

Conflicts of interest

The authors have no conflicts of interest to declare.

References

[1] http://news.chosun.com/site/data/html_dir/2018/02/16/2018021600671.html. Accessed 11 January 2018.
[2] http://www.dailynk.com/korean/read.php?cataId=nk00100&num=110161. Accessed 17 November 2017.
[3] http://www.rfa.org/korean/commentary/ae40d0dcc6b0-ce7cb7fc.html. Accessed 21 November 2017.
[4] Park SW. The age of artificial intelligence, trans human strategy. Science & Technology Policy. 2016; 26(11):38-41.
[5] https://ko.wikipedia.org/wiki/%EC%95%8C%ED%8C%8C%EA%B3%A0. Accessed 18 January 2018.
[6] http://www.itworld.co.kr/news/54798. Accessed 13 January 2018.
[7] Kim DY, Lee J.H, Park MH, Choi YH, Park YO. Trends in brain wave signal and application technology. Electronics and Telecommunications Trend.2017; 32(2):19-28.
[8] http://www.etnews.com/20170504000119. Accessed 21 November 2017.
[9] http://www.ndsl.kr/ndsl/search/detail/report/reportSearchResultDetail.do?cn=TRKO201700005055. Accessed 21 November 2017.
[10] Eun Y, Park KJ, Won M, Park T, Son SH. Recent trends in cyber-physical systems research. Communications of the Korean Institute of Information Scientists and Engineers. 2013; 31(12):8-15.
[11] Yongsoo L. Problem of definition on mixed reality and its alternative, and relationship of virtual/augmented reality. Korea Design Knowledge Journal. 2015; 34:193-202.
[12] https://crpc.kist.re.kr/common/attachfile/attachfileNumPdf.do?boardNo=00006437&boardInfoNo=0022&rowNo=1. Accessed 21 November 2017.
[13] https://www.dropcatch.com/Domain/sersc.org. Accessed 21 November 2017.
[14] Hur CH, Kim SP, Kim YS, Eom JH. Changes of cyber-attacks techniques and patterns after the fourth industrial revolution. In international conference on future internet of things and cloud workshops 2017 (pp. 69-74). IEEE.
[15] Yang BS. Development direction and implications of virtual reality / augmented reality technology. Software Policy & Research Institute Publishers, Sungnam-si; 2017.
[16] Park SW, Choi JH, Jin SA, Lee JY, Kim EA, Kim JH. An exploration of science and technology policy issues in response to the rise of transhumanism. Future Media Publishers, Sejong-si; 2016.

[17] https://www.boannews.com/media/view.asp?idx=51701. Accessed 10 January 2018.
[18] Kim, S. Re-examination of strategy: centering around the role of human and insight in strategic studies. Korean Journal of Military Art and Science. 2017; 73(3):153-96.
[19] Applegate SD. The principle of maneuver in cyber operations. In international conference on cyber conflict 2012 (pp. 1-13). IEEE.

Sin Gon Kim received his M.S. degrees in Defense Management Studies from National Defense University, Seoul, Korea in 1996. He is currently a Maintenance Officer (Colonel) at RoK Airforce and attending a Doctoral Course in Korea. His research interests are National Defense Acquisition, Information System, Cyber Warfare, Military Studies.
Email:saintjo7841@naver.com

Sang Pil Cheon received his M.S. degree in Mechanical Engineering from Yonsei University, Seoul, Korea in 1994 and Ph.D. degree in military studies from Daejeon University, Korea in 2015. He is currently a Visiting Professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are Cyber Warfare, Aircraft Maintenance, System Acquisition Strategy.
Email: 69202@naver.com

Jung Ho Eom received his M.S. and Ph.D. degrees in Computer Engineering from Sungkyunkwan University, Suwon, Korea in 2003 and 2008, respectively. He is currently an Associate Professor of Military Studies at Daejeon University, Daejeon, Korea. His research interests are Information Security, Cyber Warfare, Network Security.
Email:eomhun@gmail.com