특집 03

A Study on the Improvement for Military Cyber Protection Technology in the 4th Industrial Revolution

Chulhyun Park · Jingul Kim · Daesol Kim (Korea Army Academy at Youngcheon)

목 차

1. Introduction

1.1 The 4th Industrial Revolution and Defense Cyber Protection System

The core technologies of the 4th Industrial Revolution are known as AI(Artificial Intelligence), IoT(Internet of Things), Big Data, Cloud Computing, 3D printing and Cyber Security. This heralds the era of uncertainties beyond the predictable age based on the Hyper-connectivity & Super-intelligence through the distribution and convergence of global data, and self-evolving technologies. Meanwhile, Ju said that various hacking attacks, resulting from the vulnerability of convergence of these key technologies or newly-developed weaknesses, are taking place throughout the world and will continue to rise in the future. He suggested cyber attack patterns such as Ransomware, the increase in the number of attacks, and the diversification of attack methods. One of the biggest concerns in the age of Hyper-connection is the information security threat such as voluntary and involuntary information leakage. The Ministry of National Defense is also trying to conform to the 4th industrial revolution through Cloud Computing and Big Data, starting with the establishment of Defense Integrated Data Center and the launch of Military IoT(M-IoT). As the intelligence and communication environment is becoming more sophisticated, it has become a movement to build a huge network integrating current command and control systems, wired and wireless communication networks and weapon systems software linked to them. Various information assets that are distributed and operated by organizations and systems will be integrated into Cloud Computing systems in application, server and information service environment. In addition, applications and information services will evolve into a single sign-on environment, and the network environment will expand and integrate with IP(Internet Protocol) technology. However, as the defense networks expand and become automated, the vulnerabilities and the number of targets that the enemy can attack are increasing. In particular, the hacking attack in August 2016 indicates the vulnerability of current cyber protection technologies, which resulted in an attack on the vulnerability of connections to the network via the antivirus update server between the Internet and the Intranet. Now, in operating the information and communications system, such as a massive chain of defense networks, Cyber Protection Technology also needs to establish a system for mutual monitoring, identifying vulnerabilities and warning. Accordingly, this paper analyzes the factors of the 4th industrial revolution that will be applied to the defense information and communications system in the future and the vulnerable elements that can be caused by them, and presents directions for operating and enhancing the Cyber Protection Technology.

2. Current Status

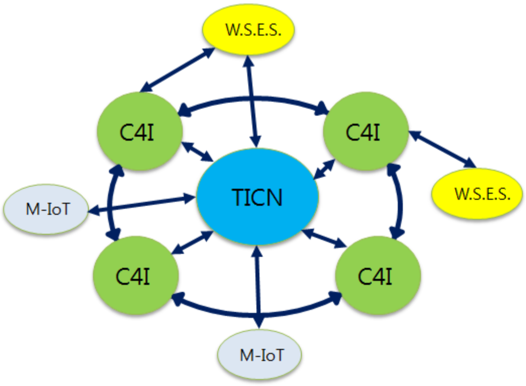
2.1 Development of Defense Big Data and AI Technology

Big data technology, one of the core technologies of the 4th industrial revolution, is expected to be gradually applied to the military. According to Han and Kang, U.S. military spends more than $ 250,000 a year on Big Data in the defense sector, using it to prepare for the enemy's cyber attacks as well as physical attacks(In addition, they suggest using Big Data to military promotions and CRM(Customer Relationship Management) through SNS analysis, as well as utilizing it to inventory management of military supply items, and to help troubled soldiers). They said the ROK military is also collecting data on North Korean forces and analyzing their patterns precisely to predict and prepare for their military action.

The ROK military is operating the Defense Integrated Data Center in the field of non-weapon systems, which integrating Army, navy and air force service systems into one. It was built on the defense network which is a peace time network in the military. In particular, it has a search function similar to the knowledge portal search function, which is commercially available in the Internet network, and is continuously upgrading functions for database extension and convenience enhancement. In the field of weapon systems, the functions are applied to C4I System (Command, Control, Communications, Computer and Intelligence System) to support commanders' decisions in case of emergency by collecting and analyzing real-time data from each individual soldier to higher units. In other words, after processing the received data into useful information, it is expected to be automated to derive analysis factors for decision making from given information, and to give priority to them. We also expect that the uncertainty of the battlefield will increase more as the number of cases is generated and the prediction is repeated by analyzing past data to support the current optimal decision-making process. Moreover, military data and information collected at strategic levels, when they are linked with national central agencies, can also support the Chief Executive Officer's decision, which means that a huge amount of data will circulate in and out of the military. However, data to be distributed might include many sensitive data such as personal information and tactical situations, which are directly related to military security issues. Although the military has been preparing security measures using encryption and authentication system for sensitive computer files including military documents, systematic information protection systems such as masking of a large amount of data are not established yet. Futhermore, the military has not established any countermeasures in cases where sensitive information (personal information, confidential information, etc.) is predicted by deliberate tracing methods which work on intentionally excluded sensitive date when information from more than two objects is provided in externally distributed documents, PC files and mobile transmission. In other words, as the decision support system becomes more automated, more information will be circulated, and if a little bit of the sensitive information is exposed, the enemy will be more easily informed of our intention.

2.2 Development of Hyper-Connectivity and IoT Technologies

Hyper-Connectivity in the 4th Industrial Revolution will be applied to support the optimal decision-making by interlinking the core information and communication networks of the military such as the tactical network currently being built, C4I systems, the weapon systems software and the Weapon Systems Embedded Software. It is also believed that the area will include the military IoT(M-IoT) which is currently initiated. We can expect the future tactical communication system to be mutually interlinked as shown in Fig. 1. Shin and Kim suggested that there are many areas in which M-IoT can be introduced such as recruitment training, military barrack, surveillance, reconnaissance, accident prevention, military logistics innovation and military



* W.S.E.S. : Weapon Systems Embedded Software

(Fig. 1) Future tactical communication system medical system. Among them, it was judged that recruitment training and the improvement of military barracks would be the first. They also predicted that wearable devices for small-scale special forces would be used in the early stages of the military strategy to increase combat capability awareness and combat power by utilizing weapon systems and two-way data systems, and the next stage will be extended to the large-scale battle systems that include C4I systems. The ROK military is extending the scope of M-IoT by launching the Wearable Health Care System using wearable devices, the Logistics Management System, etc. They are also building TICN(Tactical Information Communication Network) composed of complex sub systems such as high-capacity wireless transmission systems, small wireless transmission systems, telecommunications systems, combat radio systems, tactical mobile communication systems and network control systems. As a core tactical network of ROK armed forces, TICN supports communications from a small unit to large troops. It can be utilized for real-time information distribution and optimal command determination in conjunction with the C4I system or the individual battle information system to be deployed in the subsequent IoT format. However, as "Security is a chain of various cyber security capabilities. The overall level of security is determined by the weakest parts of the chain.", vulnerabilities exposed in the weakest parts of the network can be directly targeted to enemy cyber attacks. Attacks and risks against tactical networks are shown in Table 1.

And threats of IoT linked with tactical networks, such as increased threat of the illegal system access and utilization by unauthorized users, increase in the possibility of compromising confidential information and difficulty in verification of accuracy and reliability of information. Also, Weapon Systems Embedded Software that is linked to tactical networks and M-IoT is vulnerable to its

〈Table 1〉 Risk factors for tactical networks

Main attacks		Degree of vulnerability	Effect	Degree of Risk	Counter −measures
Passive	Eavesdrop	Low	High	Low	Cryptography
	Traffic Analysis	High	Low	Medium	Traffic Obfuscation
Active	Dos	Low−High	High	Low−High	Layer Specific Mechanism
	Masquerade	Low	Very High	Medium	Trust System Cryptography
	Modification	Low	High	Low	Cryptography
	Jamming	High	High	High	Anti−Jamming Cognitive Radio

Common defense methodology : Cryptography, Authentication, Tunneling, Anti−Jamming, Cross−layer Approach, Policy−based Management own defects and external attack due to insufficient Maintenance Management compared to its importance. In particular, the secure coding is not applied, which can be the most realistic alternative to minimizing infringement caused by its own vulnerability during software development. Threats to Weapon Systems Embedded Software including a total of 59 vulnerable factors have been studied in the categories of software modulation, software implementation, hardware external, hardware terminal, hardware component intrusion, hardware replication, data, visual information, user interface, system access and password implementation. These factors act as links to security vulnerabilities, causing significant damage to allies in case of emergency. An example of this is the failure of a timely interception due to an embedded software defect of an interceptor missile against an enemy ballistic missile attack.

2.3 Human resource training and education

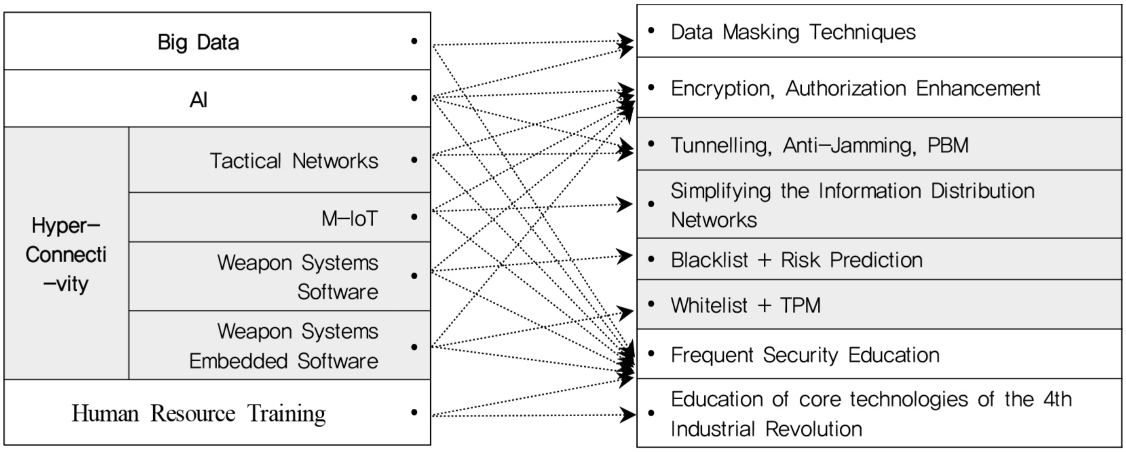
The lack of professional personnel and professional education programs to carry out cyber protection in the military is an ongoing problem. Intermediate technical education for Cyber Warfare or Intelligence Protection is taught at each military Intelligence-Communications School only for commissioned officers who are in the branch of Communications. Seo et al. argued that it is difficult to say that the officers were educated as Cyber Warfare professionals only by completing the education because those schools only provide the level of understanding the concept of Cyber Warfare and Intelligence Protection. Thus, they emphasized the importance of the education in basic education institutes that include universities. On the other hand, Eom argues that cyber security education in S. Korea is mainly centered on basic education institutes, and the intermediate and higher technology education that can improve the cyber security capability is not systematically implemented. That is, cyber protection education should be continuously managed from basic education institutes such as universities, private and public agencies to practical cyber training institutes. Particularly, as the age of the 4th Industrial Revolution comes, for Cyber Warfare experts have to cultivate their ability to deal with Big Data analysis, IoT and artificial intelligence, both the basic and the higher technology curriculum should be strengthened. Eom et al. suggest that Cyber warriors in the defense sector should be differentiated and specialized as compared to Cyber security experts in the private sector, because the Cyber Warfare is conducted in conjunction with physical warfare. They also said that cyber warriors in the defense sector should have specialized expertise and knowledge in defense policies, military strategy, operations, tactics and cyber attack & defense skills.

3. Improvement

We derived cyber protection technologies required during the 4th Industrial Revolution era through several practical discussions and research from January to May 2017, participated by the personnel in charge of Information Planning in each military service and university professors. As a result, the core technology elements of the 4th Industrial Revolution and the required cyber protection technologies were intersected and matched as shown in Figure 2. Details are discussed in the following sections.

3.1 Improvement for Defense Big Data and AI Technology

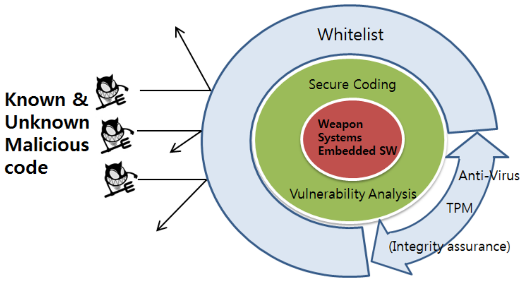
As described in the previous chapter, for the military's decision-making system is automated and the vulnerability further increases, Park et al. suggested a classification method which can identify and deal with high-risk information using the disclosure risk measure. Data can be categorized into micro data including private data for individuals, households and businesses, and macro data such as division tables or spreadsheets provided to government agencies, academics and research institutes. Especially, the Big Data technology to be applied to the military has to support the commander's determination by distributing and processing real-time (or near real-time) micro data, so we should consider the risk of direct object exposure or deliberate reasoning in the process. Thus, we need to classify and manage the data in accordance with exposure risk in case the sensitive information is inferred by acquiring part of the data using social engineering techniques. The higher the risk of exposure, the more protective measures should be taken before providing information to the outside. In this regard, data protection techniques such as anonymization, sample provisioning, population size restriction, concealment, data exchange, noise addition, blurring, Micro-Aggregation and


Big Data
AI
Tactical Networks
M-IoT
Hyper-Connecti-vity
Weapon Systems Software
Weapon Systems Embedded Software
Human Resource Training
Data Masking Techniques
Encryption, Authorization Enhancement
Tunnelling, Anti-Jamming, PBM
Simplifying the Information Distribution Networks
Blacklist + Risk Prediction
Whitelist + TPM
Frequent Security Education
Education of core technologies of the 4th Industrial Revolution

(Fig. 2) Operation Strategy for Cyber Protection Technology etc. have been studied. Some public institutions have applied these technologies to protect sensitive information. However, since the ROK military does not apply protection technologies as well as techniques for measuring exposure risk, it is urgent to take measures against them.

3.2 Improvement for Hyper-Connectivity and IoT Technologies

Table 1 shows Cryptography, Authentication, Tunneling, Anti-jamming, and Policy-based management (PBM) as countermeasures against tactical network threats. Shin and Kim proposed strengthening of cryptography and authentication, and simplification of information distribution network as security countermeasures against M-IoT. On the common defense methodology, these are all universal and essential security elements. Advances in the 4th Industrial Revolution have been developed by artificial intelligence systems, which automatically identifies the threat of unknown threats, but the ROK military hasn't introduced them, so the military has to rely on a lot on security system operators for the next several years. Therefore, it is very important to educate the people who operate security systems because it is known as 'the greatest enemy of security is human beings'. In other words, we have to constantly check that the security measures to be operated are in operation, and to continue to educate on the latest updates for malware information, up-to-date security patches and enhanced personnel security against social engineering attacks. In order to improve the defense cyber protection, we need to build a system to detect and block cyber threats and to monitor threat situation, abnormal status and log information throughout the system and network by adding to current integrated security control system. And the system should support identification of unknown cyber threats through comprehensive analysis using Big Data technologies. Unknown threats target both tactical networks, C4I systems, and Weapon Systems Embedded Software, so protection schemes are needed for their own characteristics. Park et al. introduced the Whitelist + TPM (Trusted Platform Module) Solution as a countermeasure against weakness of the Weapon Systems Embedded Software. Weapon Systems Embedded Software has the characteristics of being limited to specific areas of work, closed or stand-alone format and low specification in comparison to other weapon systems software, so Whitelist techniques that block unknown threats can be applied. Since the typical weapon systems software has a wider operating range than Weapon systems embedded software, Blacklist technique is applied to them rather than Whitelist technique to cope with relatively known malicious code. In this case, we need to constantly predict unknown malicious code by frequent updates and the Big Data technologies. In contrast, the Weapon Systems Embedded Software is relatively small in scope, so it is effective to apply a method that blocks all but the specific allowed executable files. Moreover, the Weapon Systems Embedded software can strengthen security by intelligently filtering malicious code at the hardware level before access control through the Whitelist. Using such techniques, we can cope with physical attacks such as hardware terminals, component intrusion and duplication. In this regard, Park et al. introduced the application of Trusted Platform Module (TPM) which is a chip type module that can block unknown attacks such as Zero-Day Attack at the hardware level. It can function as a reliable computing platform for storing cryptographic keys or passwords in nonvolatile space and providing access to storage space, integrity verification of remote hosts, reliability based communication, and providing secure communication channels. Consequently, the Weapon Systems Embedded Software can use TPM at the hardware level to ensure integrity and then apply the whitelist at the software level to enhance protection. Figure 3 shows a application of Whitelist + TPM solutions to Weapon Systems Embedded Software.



(Fig. 3) Application of Whitelist + TPM Solutions to Weapon Systems Embedded Software

3.3 Improvement for Human Resource Training and Education

Seo et al. analyzed basic fundamentals for training a Cyber Warfare expert as shown in Table 2. The analysis results show that the weight of 'Firm view of the nation' is higher than that of the Programming technique and the Basic knowledge of information security. In order to cultivate a firm view of the nation, we need to emphasize the recognition of the reality of the nation's military and the importance of cyber warfare in national security. To this end, we have to continue to educate the latest version of cyber threats and cases first in order to ensure that the students understand the international situation and the changes in cyber warfare. Second, education on cyber warfare as a part of war should be strengthened. That is, the operational training of cyber warfare at the strategic level should mainly contain a comparative analysis of competence among major countries, the use of cyber psychological warfare in war, the countermeasures against cyber attacks and related statutes (such as Tallinn Manual).

Third, cyber operations training should be strengthened, namely Cyber Attack & Defensive Operations and Network Operations. We have to train students to equip themselves with basic skills to use tactics as soldiers because war is a strategic aspect, but military operations are operational and tactical. Degree courses in Cyber warfare mainly deal with computer architectures, operating systems, 〈Table 2〉 Basic Fundamentals for Cyber Warfare experts

( ) : Weight value

1st layer(Civil, Military)	2st layer(Civil, Military)
Sense of duty (0.344, 0.376)	Firm view of the nation (0.514, 0.419)
	Ethics (0.281, 0.299)
	Challenge spirit (0.205, 0.282)
Planning Capacity (0.287, 0.213)	Programming (0.495, 0.535)
	Document Writing (0.194, 0.184)
	Basic knowledge of information security (0.312, 0.281)
Internationality (0.200, 0.211)	Global cultural awareness (0.506, 0.506)
	Foreign language ability (0.494, 0.494)
Leadership (0.169, 0.199)	Insight and judgment (0.461, 0.488)
	Cooperation (0.300, 0.189)
	Driving force (0.239, 0.323)

programming languages, information protection, digital forensics, system and web security and cyber battle exercises, which are related to technical aspects (programming, basic knowledge of information security and etc.).

Particularly, in the case of the cyber battle exercise, it is necessary to construct a training facility capable of both attack and defense, but is mainly focused on defense. Eom et al. emphasized that defense cyber warriors should conduct training in cyber training facility optimized for specific cyber domains. This is because defense related information and communication systems are constructed in various ways, such as production and transmission of national security related defense documents, communication of military confidential data, collection of key information, analysis and dissemination of information. In addition, Big Data, IoT and artificial intelligence programs should be added to both basic and upper middle class curriculum in order to meet the 4th Industrial Revolution era. For example, the basic curriculum needs to reinforce basic statistics and data analysis to deal with Big Data, and network programming and network security for the IoT. And higher education institutions such as Information-Communications Schools should supplement the process to be immediately applicable to higher-level practices than basic curricula, such as Big data analysis using toolkits, intermediate network programming and security. In order to broaden the experiences of students, we need to set up opportunities to actively participate in the Korea Information Technology Research Institute (KITRI) 's Next Generation Security Leader Course (BoB : Best of the Best), Hacking Defense Competition, etc.

4. Conclusion

Currently, S. Korea is entering the era of the 4th Industrial Revolution beyond the level of computerization and automation based on the National Informatization. Some of the technologies of the 4th Industrial Revolution are already expanding to the base of our society beyond the R&D stage, so the ROK military can not be an exception. The Ministry of National Defence is planning to build the optimal decision-making system which based on the integration of tactical networks, C4I systems, M-IoTs and the establishment of the Integrated Data Center, using the key technologies such as Big Data, Artificial Intelligence and IoT. However, as the network which implementing Hyper-connectivity & Super-Intelligence expands and becomes automated, the security vulnerabilities that can cause major disruptions to the network are increasing, which highlights the importance of cyber protection in the 4th Industry. As a result, we suggest the data masking techniques for Artificial Intelligence, and encryption techniques, enhancement of authentications, tunneling, Anti-jamming and PBM for tactical networks, encryption techniques, enhancement of authentications and simplifying the information distribution networks for M-IoTs, the Blacklist techniques + Risk Prediction technology for weapons systems software and the Whitelist techniques + TPM for Weapon Systems Embedded Software. We also provide the necessary security education for the security system operators. Additionally, as the necessary preconditions for applying these technologies, we have indicated the need for enhancing the core technical training of the 4th Industrial Revolution to improve both basic and practical skills required for the cyber warfare experts.

The expansion of the 4th Industrial Revolution makes our daily lives more convenient, but targets in the cyber space that can be attacked by North Korea are increasing. Therefore, through this study, we hope the ROK military will be interested in the proper functioning of cyber protection technology and continue to improve it. We will also investigate what should be supplemented and improved when the cyber protection technologies proposed in this paper are actually applied.

참고문헌

[1] Ju, D., What should we do for 4th Industrial Revolution and National Cyber Security?, The 4th Industrial Revolution and the National Cyber Security Policy Forum, Presidential Commission on Broadcasting and Communications / National Cyber Security Association, S. Korea, Keynote presentation, 2017.

[2] Cho, S., The Study on Threats of Information Security and Their Solutions in the Fourth Industrial Revolution, Korean security science review, Vol.51, pp.11-35, 2017.

[3] Choi. I., Defense cyber protection development direction, Weekly defense review, KIDA, S. Korea, Vol.1659, pp.1-8, 2017.

[4] Han, C. and Kang, W., The Utilization of Big Data Technologies in the ROK Army, Journal of Business Administration Research, S. Korea, Vol.9, No.1, pp.5-24, 2016.

[5] Shin, S. and Kim, Y., A Study on the Cyber Cyber-Construction and Countermeasures by Introducing IoT, KINX2016257139, ROK. Joint Chiefs of Staff, S. Korea, pp.81-84, 2016.

[6] Ha, Y., Chung, Y., Lim, Y. and Yang, H., A Study on the Development of UAVs for the Public Switched Information System in Korea, KICS, S. Korea, Proceedings of the Summer Conference, 2009.

[7] Schneier, B., Secrets & Lies, John Wiley& Sons, 2000.

[8] Ross, R. S., Managing Information Security Risk: Organization, Mission, and Information System View, Special Publication (NIST SP), 800-39, Mar. 2011.

[9] Kidston, D., Li, L., Tang, H. and Mason, P., Mitigating Security Threats in Tactical Networks, Communications Research Centre (CRC), White Paper, 2010.

[10] Park, C., An, H., Kim, S. and Bae, J., Strategies to Improve the Management System of Weapon Systems Embedded SW and to Construct its Information Security System, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.4, pp.363-378, 2015.

[11] S. Korea's Defense Acquisition Program Administration, A Handbook on the Development and Management for Weapon Systems SW, 2013.

[12] Seo, S., Oh, W. and Kim, H., Research on cyber warfare manpower training strategy for securing Defense Information System using AHP analysis, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.2, pp.109-120, 2015.

[13] Eom, J., The Improvement Plan of a Customized Cyber-Training Structure for enhancing the Capability of Cyber Security, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.6, pp.567-580, 2015.

[14] Eom, J., Lee, W. and Park, K., A Construction Plan of Specialized Cyber Training Scheme for Enhancing the Capability of Military Cyber Warriors, Journal of Security Engineering, SERSC, S. Korea, Vol.13, No.2, pp.99-112, 2016.

[15] Park, C., Kim, C., Kim, S., An, H. and Bae, J., Improvement of Personal Information Protection Level in the Military Using the Measurement of Disclosure Risk, Journal of Security Engineering, SERSC, S. Korea, Vol.12, No.6, pp.581-596, 2015.

[16] Eurostat, Manual on Disclosure Control Methods, Luxembourg, Office for Official Publication of the European Communities, 1996.

[17] Techtarget Network, http://whatis.techtarget.com/definition/policy-based-management, 2011.

[18] Network Times, Whitelist Security, 153-162, 2010.

[19] Choi, J., Park, W. and Park, C., A Framework of Secure Access to iSCSI Network Storage based on TPM, KCC2009, Vol.36, No.1D, pp.5-9, 2009.

저자약력

박철현

이메일 : kmanp@cnu.ac.kr

- 1999년 육군사관학교 물리학 (학사)
- 2003년 국방대학교 무기체계학 (석사)
- 2016년 충남대학교 수학통계학 (박사)
- 2016년~현재 육군3사관학교 컴퓨터공학/사이버전학과 조교수
- 관심분야 : 큐잉이론, 시뮬레이션, 소프트웨어공학, 사이버전 등

김진걸

이메일 : c15247@gmail.com

- 2007년 육군사관학교 전산학 (학사)
- 2015년 미 USC 컴퓨터공학 (석사)
- 2015년~현재 육군3사관학교 컴퓨터공학/사이버전학과 강사
- 관심분야 : 시스템/네트워크 보안, 운영체제, 사이버전 등

김대솔

이메일 : a1088342256@gmail.com

- 2010년 육군사관학교 프랑스어학 (학사)
- 2016년 프랑스 ISEP 정보공학 (석사)
- 2016년~현재 육군3사관학교 컴퓨터공학/사이버전학과 강사
- 관심분야 : 데이터마이닝, 보안모델링, 사이버전 등