KOREA INSTITUTE FOR DEFENSE ANALYSES

KIDA Brief

NO. 2021-1

KIDA Brief provides publicly available summaries of research projects and analysis conducted at KIDA.

Mid- & Long-Term Developments in Joint Command and Control, Communication Systems

AHN, Byung Oh
Military Development Research Center

Background and Purpose

☐ **This research serves as a preliminary study for the Joint Chiefs of Staff's plans for developing the next-generation Joint Command, Control & Communication (C3) systems.**

○ In its Defense Information System Modernization Basic Plan, the Ministry of National Defense (MND) has called for a digitized, "smart" deployment of military capabilities based on the most cutting-edge ICT innovations.

○ The Joint Chiefs of Staff is currently developing a comprehensive plan for developing joint command & control, communication systems, within the policy directions laid out by the MND.

○ This research suggests development directions for the establishment of a joint command and control and communication systems based on the 4th industrial revolution technology.

Research Results

☐ **This research charts the future trajectory for the development of applying Fourth Industrial Revolution technologies to C3 systems.**

○ The future joint operation will emphasize the establishment of an intelligent-based operational environment to perform integrated operations in all areas, and will require real-time connectivity and interoperability for all battlefield elements.

- Thus, joint command & control and communications systems will have to be developed in the direction of more advanced real-time, hyper-connected, intelligent and interoperable, accounting for the latest developments in Fourth Industrial Revolution technologies and changes in the strategic environment.

○ The Way Forward.

- Build an integrated battlefield mobile operation environment to ensure joint coordination
- Improve the intelligent C4I system to a system that focuses on creating a battlefield artificial intelligence ecosystem
- Develop the combined C41 system for the Rep. of Korea military, in sync with the U.S. military's development of the Mission Partner Environment (MPE) project.
- Re-construct cybersecurity systems from the perspective of integrated security, proactively anticipating changes in the security paradigm.
- Enhance cybersecurity across all life cycles of weapons systems, in sync with the U.S. military combined C4I system environment and Risk Management Framework (RMF).

In the future battlespace, how will command & control (C2) proceed over joint operations? The answer lies in an "intelligent-based operational environment," one where the technologies of the Fourth Industrial Revolution can be fully utilized. Within such an environment, the C2 system will link efforts across space and time, leading to more effective force deployment and operational efficiency. Within the intelligent-based operational environment, all battlespace elements will be networked, and copious amounts of data will be collected, analyzed, and processed in real-time. This, in turn, will lead to closer integration of manned and unmanned battle systems. Each battlespace element will be intelligent to a certain level by having computing and communication capabilities, and the connectivity between them will be greatly expanded. Future command, control, and communications (C3) systems will connect the battlefield elements in all areas through an integrated network. Moreover, improvements in connectivity and interoperability will also materialize across data storage & analysis, decision-making support, and joint C2 systems. This research intends to discuss an in-depth analysis of future development in C3 systems.

Because of the Fourth Industrial Revolution, recently the technological environment is becoming hyper-connected, more advanced real-time and intelligent. This environment is marked less by individual technological growth, but more by technological integration. Big Data and Artificial Intelligence (AI) services are built within the cloud environment, and the Internet of Things (IoT) technologies enable the collection of a wide range of data; moreover, the 5G network provides timely services to users. AI technologies have become embedded in the Big Data platforms, and platform capabilities and applied services have been incorporated into cloud computing; this data is now distributed on a 5G network. The Korean military's intelligent-based operational environment will be realized based on these technological developments.

The strategic environment is also changing. The U.S. military is currently building the Mission Partner Environment (MPE) to improve the combined operations environment. One aspect of this project is to strengthen cybersecurity, and for this purpose, the U.S. is demanding that its allies also apply the Risk Management Framework (RMF) to their respective military procurement and synchronization efforts. As similar demands (i.e., the application of the MPE and RMF) are likely to be made on the Korean military, the appropriate response to such a request will have to be issued. Now is the appropriate time for developing an effective strategy for harnessing developments in C3 systems, in light of the application of Fourth Industrial Revolution technologies and changes in the strategic environment. Moreover, real-time interoperability among all battlespace elements is a prerequisite for enhancing jointness, and ought to be an indispensable element when developing systems either individually or in sync with one another. However, currently, each service branch is establishing its separate environment; as a result, inefficiencies with respect to limited jointness, overlapping investments, and increased costs are likely to hamper operational effectiveness. Thus, it behooves the Joint Chiefs of Staff to strengthen joint-level oversight and planning capabilities, setting the stage for a joint intelligent platform. This research provides the following five recommendations.

First, to ensure jointness, a mobile battlespace environment enabling access of multiple heterogeneous mobile network ought to be created. Under the status quo (i.e., each service going its separate way), inevitably the terminals, equipments and services are left unstandardized across the armed services. This, in turn, will lead to complications in the operational environment. The military ought to standardize the battlespace mobile environment across all branches. Regular, day-to-day administrative tasks will be conducted on a civilian, commercial mobile network, considering the fact that both civilian and military working environments make use of fixed facilities. On the other hand, tactical tasks are mobile by nature, and ought to consider the limited frequency band of the military. Because of this reason, there needs to be an increase in connectivity with the Tactical Information Communication Network (TICN), and improvements in survivability are also called for. Ultimately, 5G technologies and individual mobile networks will have to be integrated so that individual vehicles can support multiple telecommunications networks. And edge computing capabilities will need to be provided so that individual vehicles can provide intelligent data collection and analysis services to front-line units. Additionally, integrated telecommunications RF modules that can minimize the use of personal electronic devices will have to be widely adopted. And standardized application services that can effectively coordinate multiple applications on a given single device will have to be provided.

Second, intelligent C4I systems need to be upgraded with an emphasis on the creation of an inter-service battlespace AI ecosystem. The Korean Joint Command and Control System (KJCCS) will have to improve its battlespace situational awareness capabilities, strengthening the requisite decision-making support capabilities. To this end, a shift to an intelligent C4I system is called for, in light of innovations in the operational and technological environments. AI technologies can be integrated into developing battlespace management capabilities that guarantee a high level of interoperability across the service branches. These capabilities, furthermore, will have to encompass the unique operational environment of each military branch. To this end, military-use data ought to be integrated into the cloud platform, and the platform will have to analyze the data using machine-learning techniques. Data analysis results will then be tailored to meet the needs of different users. The Joint Chiefs of Staff, in this vein, ought to provide an joint intelligent platform uniquely devote to battlespace management. Each service branch will need to revise its C2 information sharing concept, aligning such efforts with the work carried out at the Joint Chiefs of Staff level. The KJCCS also can benefit from a technological upgrade using such a platform.

Third, Korea's Allied Korean Joint Command & Control System (AKJCCS) system needs to be developed in sync with the progress made on U.S. military's MPE project. Developments in the U.S. military's MPE project ought to inform the Korean military's interoperability structures and combined C4I systems; useful precedents will also be offered by North Atlantic Treaty Organization (NATO) and Australian armed forces cases. Primarily, after the transfer of wartime operational control (OPCON) from the U.S. to the Korean military, the operational concept will have to be revised so that AKJCCS can function as the main system for Korean military-led combined operations. In this vein, interoperability in information and capabilities will have to be expanded between the U.S. and

ROK forces. In the short-term, combined battle domain governance that encompasses standards for technology, data and information sharing, and RMF will have to be set up, with the key structural assumption being the bilateral relationship between the U.S. and ROK forces. In the long run, other nations' militaries can also take part in this partnership.

Fourth, in preparation for changes in the cyber-security paradigm, there needs to be a rebuilding of the cyber defense systems, from the perspective of integrated security. This is to respond promptly to complex cyber threats. Cutting-edge technologies ought to be embedded in a flexible and rapid cyber defense posture. What such a posture necessitates are analyses of the safety of pre-existing infrastructures, as well as advancements in cyber defense, collective cyber situational awareness and threat response systems; ultimately, militaries ought to be able to detect irregular activity across all domains.

Lastly, accounting for the U.S. military's implementation of RMF, cybersecurity ought to be enhanced throughout the life cycles of weapons systems, in sync with the U.S. military combined C4I system environment and Risk Management Framework (RMF). The U.S. military requires the application of RMF within the MPE context; if relevant criteria are not satisfied, however, synchronizing the two countries' systems is likely to be a tough challenge. Currently, the Ministry of National Defense (MND) is reviewing its indigenous cybersecurity structures conducive to the RMF. Thus, the Joint Chiefs of Staff must also have adequate measures with respect to conducting current operations. As for this issue, it may be necessary to proceed with the developments in cybersecurity systems in close alignment with the measures taken by the U.S. military. After all, the Korean military also needs the RMF, to enhance cybersecurity across all life cycles of weapons systems. On the American end, there need to be improved system protection and control elements, more synchronization of risk management and security measures at the software development stage. With respect to cybersecurity systems, the concept of RMF will have to be used to overcome the current limitations of applying the latest cutting-edge technologies.

** The views expressed in this paper are those of the participants (Ahn, Byung-Oh, Pyeon, Do-Hoo, Ko, Hyun-Ho, Hong, Su-Min) of the research project **"Research on Developing Next-generation Joint Command, Control & Communication (C3) systems"** conducted at KIDA in 2020, and do not represent or reflect the official position of Korea Institute for Defense Analyses.*