

NEW COMMANDER, OLD WIRING: KOREA'S UNTESTED OPCON CERTIFICATION

BY DAVID F. HELVEY AND KANGKYU LEE

David F. Helvey *(david@meridiusstrategies.com) is Distinguished Fellow for Defense Strategy and Indo-Pacific Security at the Institute for Security and Technology. He previously served as a senior official in the US Department of Defense, with responsibilities for Indo-Pacific and Euro-Atlantic security; he led the US side of the Korea-US Integrated Defense Dialogue from 2011 to 2015 and was responsible for Korea policy from 2017 to 2021. The views expressed here are his own and do not represent the views of the US Department of Defense.*

Kangkyu Lee *(kang@securityandtechnology.org) is Deputy Director for Technology and Geopolitics in Asia at the Institute for Security and Technology and a Ph.D. candidate at Georgia Tech's Sam Nunn School of International Affairs. He was Pacific Forum's Resident Korea Foundation Fellow in 2020.*

For two days in August, as part of the Ulchi Freedom Shield exercise which opened at reduced scale and closed six days early, the US-Republic of Korea alliance tested whether the Republic of Korea Armed Forces could command the combined force. In the end, the American four-star retained command for both days. ROK command of the combined defense on the Korean Peninsula is the first gap under the certification the US and ROK defense ministers will need to take up at the next Security Consultative Meeting. That meeting, normally held in the fall, has slipped to early 2027, officially over scheduling, with the two ministers meeting in Washington in December ahead of it. The second gap is physical: the network the future headquarters will operate through. It is being rebuilt, and the rebuild is not expected to finish until at least 2029, well after the projected date for the transfer of operational control to the ROK. The third concerns cyber operations. Across 14 years of alliance documents on cyber cooperation, not one formalizes that cooperation with language authorizing how the future combined force would command and control those operations. In the public record at least, the Combined Forces Command (CFC) a South Korean general would inherit has no cyber chain of command at all.

These gaps are consequential. The certification process is supposed to determine not only whether the ROK possesses the military capabilities required to lead the combined defense on the Korean Peninsula, but also whether the future combined headquarters can perform its wartime missions under the command arrangements that will exist after transition.

In 2014, the allies abandoned the 2015 transfer target date and agreed instead to a conditions-based approach. The following year, they adopted the Conditions-based Operational Control Transition Plan. The logic was straightforward: transition would occur only when the military capabilities, command arrangements, and security conditions necessary to sustain effective deterrence on the Korean Peninsula were in place. In short, transition would not degrade the Alliance's ability to deter war and, if necessary, to fight and win one.

In 2018, the defense ministers approved the future command structure and directed an Initial Operational Capability certification for 2019, with subsequent certifications of the future command's operational capability to fully perform its wartime missions.

The focus on wartime missions means that the combined headquarters does not need to *own* every capability it employs. Some will remain national; some will be provided in support of CFC; others will depend on authorities outside of CFC. What matters operationally is whether the commander can reliably obtain, integrate, and employ those capabilities to deliver the effects necessary to meet mission objectives. This is especially important for capabilities or authorities that remain under exclusive US control.

The allies have made considerable progress in building the military capabilities required for transition. But the command being certified is not simply today's CFC with a South Korean general at the top. It is an entirely different set of command relationships.

The rewiring problem

Foremost among the things the transfer changes is the top job: the 50th communiqué of 2018 reaffirmed that a South Korean four-star would be commander and an American four-star the deputy. Yet, in the same sentence, the ministers "decided to maintain" the structure around it. Inverting the commander and deputy while maintaining the extant structure did not resolve how the combined force would integrate within that structure, and the ministers knew it. At the same meeting, they signed and endorsed four further instruments, among them Terms of Reference for relationships among the Joint Chiefs,

United Nations Command, and CFC. According to then-Minister of National Defense Ahn Gyu-back, the future command would rest on six combined component commands, whose conversion into standing organizations is underway. None of the four documents is public, there is nothing in the public record linking any of the four to a cyber layer, and the ROK has not indicated that cyber will be included among the six combined component commands.

The future CFC will function on a network that has not yet been completed. The Allied Korea Joint Command Control System is undergoing its first performance upgrade in a decade, a program expected to run through 2029 and described as so sweeping that it is tantamount to new development. Given that the projected dates in circulation for transfer are either 2027 or 2028, a South Korean commander would assume command well before the network the headquarters is expected to operate through is finished. The ministers are being asked, in effect, to certify a headquarters against a baseline that does not yet exist.

What, then, did this year's assessment actually consist of? The summer Ulchi Freedom Shield operated as a two-day Command Post Exercise, with the American four-star retaining command throughout. The assessment thus skipped the one reversal the transition is supposed to be about: at no point in the 2026 exercise did an American deputy answer to a South Korean commander. To be fair, the allies rehearsed that reversal in 2019 and 2022, but those rehearsals ran on the old wiring. The six component commands were not yet standing organizations, and no cyber command existed in the design.

Where cyber never meets command

Across 55 US-ROK Alliance documents, running from the 43rd communiqué of October 2011 to the 57th of November 2025, not one passage contained cyber-cooperation content with explicit language defining command relationships or specifying operational control. Through 2021, the two governments put out roughly two of these documents a year. From 2022 they put out just under eight, and in 2023 and 2024 they wrote more about cyberspace than they ever had. But, it appears, the two work streams never meet.

The clearest proof is the founding document itself, in October 2014. The 46th communiqué confined cyber to a single paragraph, opening with a reaffirmation of the importance of "the protection of, and access to, the space and cyberspace domains." In the same document, the ministers decided to implement the conditions-based transfer to a ROK-led defense on the Korean Peninsula. Eleven years on, the 57th communiqué of November 2025 gives cyber cooperation just two sentences. They come well after the transition plan, with its pledge to certify in 2026. Cyber is an afterthought.

Only four documents come close to uniting the two work streams. On the declaratory side, the 50th communiqué of 2018 pledges information-sharing on the reorganization of the two "respective cyber commands," and the 52nd communiqué of 2020 follows with a need for "exchanges" between them. Neither allocates authority, tasking, support, or subordination. On the exercise side, a January 2025 tabletop exercise and TACHYON ECHO 25-2 in July 2025 rehearsed nominating and assigning effects across the commands: the so-called "auction." The communiqués use the vocabulary of command but assign nothing. The readouts describe the procedure in detail but never use the vocabulary. In other words, the Alliance appears to have built the mechanism in a readout but never wrote it into the documents the certification process is supposed to assess.

The absence of a publicly defined cyber command relationship does not necessarily mean the Alliance lacks procedures for operating in cyberspace. Some of the most sensitive command arrangements appropriately remain outside the public record. The problem for certification is narrower: whether those procedures have been incorporated into the future command arrangement and demonstrated under the conditions in which they would actually be used.

Cyber operations make the issue particularly difficult because command, support, and authorization are separate questions. A South Korean four-star may command a combined operation while a capability needed to support that operation remains under US control and the approval authority to deliver a particular cyber effect remains with the US chain of command. There is nothing inherently unworkable about such an arrangement. But the relationship has to be defined, understood, and exercised before a crisis exposes its seams.

That is what the certification process should test: Can the South Korean commander identify a required cyber effect and obtain it through the future command structure? Does the American deputy have a defined role in translating that requirement into US support? Are the national and combined authorities sufficiently clear that an operational request can move at the speed of relevance? And can the headquarters integrate the effect across domains?

These are not arguments against transition. But the more responsibility Washington expects Seoul to assume for deterrence and defense on the Peninsula, the more important it becomes to establish how the future South Korean commander will access US capabilities essential to the combined defense. The 2026 National Defense Strategy captures the underlying bargain: South Korea should assume primary responsibility for deterring North Korea, with critical but more limited US support. The command architecture has to make that support operational.

Certifying the right thing

The three gaps do not argue against transition; they argue for applying the logic of a conditions-based transition to the command arrangement itself.

Before certifying, the allies should demonstrate three things: First, put a South Korean four-star in command and the American in the deputy role during the certification exercise, with operational decisions and requests for support flowing through the future structure. Second, identify the critical capabilities on which the future headquarters will depend and exercise the mechanisms through which the commander will access them. Third, exercise requesting, authorizing, integrating, and assessing cyber effects when the South Korean commander leads and American capabilities provide support.

The alliance does not need another condition for transition; it needs to ensure that certification actually measures what is intended: a combined headquarters capable of commanding in wartime under its future command relationships.

The Pilot *commentaries and responses represent the views of the respective authors. Alternative viewpoints are always welcomed and encouraged. Please write to rob@pacforum.org for more information on how to contribute.*