

XXXVI

**Impacto de la
transformación digital
en la gestión de la
ciberdefensa nacional: Un
análisis prospectivo del
Comando Conjunto de las
Fuerzas Armadas del Perú
(2026-2030)**

Ronald Leonardo Güisa Bravo

Impacto de la transformación digital en la gestión de la ciberdefensa nacional: Un análisis prospectivo del Comando Conjunto de las Fuerzas Armadas del Perú (2026-2030)

Ronald Leonardo Güisa Bravo

RESUMEN

El presente capítulo examina la evolución y el impacto de la transformación digital en la doctrina y operatividad del Comando Conjunto de las Fuerzas Armadas (CCFFAA) del Perú, analizando los desafíos críticos para el periodo 2026-2030. A través de una metodología de revisión narrativa descriptiva y prospectiva, se evalúa el estado actual de los sistemas de mando, control, comunicaciones y computación (C4I), identificando la necesidad urgente de fortalecer la ciber-resiliencia, la soberanía tecnológica y la interoperabilidad intersectorial frente a amenazas híbridas emergentes. La investigación subraya que la transformación digital no constituye únicamente una actualización técnica, sino una metamorfosis cultural y estratégica fundamental para garantizar la estabilidad nacional. Se identifican como factores críticos la automatización mediante inteligencia artificial, la protección de infraestructuras críticas y la imperativa necesidad de gestionar el capital humano especializado. Finalmente, el trabajo propone que, para consolidar un sistema de ciberdefensa autónomo, el CCFFAA debe priorizar una arquitectura de confianza cero, fortalecer la cooperación estratégica con el sector privado y actualizar continuamente sus protocolos ante tecnologías disruptivas. Se concluye que el éxito en el mediano plazo dependerá de la capacidad institucional para transitar hacia un modelo de defensa proactivo y resiliente que asegure los intereses vitales del Estado peruano en un entorno geopolítico caracterizado por la creciente competencia en el ciberespacio.

Palabras clave: ciberdefensa, transformación digital, CCFFAA, seguridad nacional,

amenazas híbridas.

Introducción

La aceleración vertiginosa de las tecnologías disruptivas ha reconfigurado radicalmente el paradigma de la seguridad internacional. En el contexto global actual, el campo de batalla ha trascendido las fronteras físicas para consolidarse en el ciberespacio, reconocido hoy como el quinto dominio de la guerra, junto a la tierra, el mar, el aire y el espacio exterior. Esta transición no es meramente técnica; representa una mutación profunda en la naturaleza del conflicto, donde la información, la conectividad y la capacidad de procesamiento de datos se han convertido en activos estratégicos decisivos. Los actores estatales y no estatales emplean tácticas híbridas que aprovechan las vulnerabilidades digitales para socavar infraestructuras críticas, desestabilizar la paz social y comprometer la soberanía nacional sin necesidad de un enfrentamiento convencional.

En el escenario nacional, el Perú se enfrenta al desafío de adaptar sus estructuras de defensa ante este panorama volátil. El Comando Conjunto de las Fuerzas Armadas (CCFFAA) opera actualmente en un entorno donde la transformación digital es una exigencia ineludible, alineándose con la Política Nacional de Transformación Digital (PNTD) que busca modernizar el Estado para atender las necesidades del ciudadano y garantizar la seguridad digital. No obstante, la gestión de la ciberdefensa dentro de las Fuerzas Armadas requiere una armonización profunda entre la doctrina militar tradicional y la agilidad de los ecosistemas digitales modernos. La capacidad del CCFFAA para integrar sistemas interoperables y fortalecer su ciber-resiliencia es fundamental para enfrentar amenazas que, para el 2026, ya han demostrado una sofisticación sin precedentes.

La importancia de abordar este fenómeno durante el periodo 2026-2030 radica en la convergencia de dos factores críticos: la aceleración tecnológica exponencial, impulsada por la integración de la Inteligencia Artificial (IA) en sistemas de combate, y la creciente inestabilidad geopolítica en la región sudamericana, donde la competencia por la hegemonía digital y el control de datos críticos se intensifica. Ignorar esta evolución no solo supone un riesgo para la operatividad de las instituciones militares, sino que expone a la nación a vulnerabilidades sistémicas que podrían comprometer su capacidad de respuesta ante desastres y amenazas a la seguridad interna.

Bajo estas premisas, el presente estudio tiene como objetivo fundamental evaluar cómo las capacidades derivadas de la transformación digital impactarán significativamente la gestión estratégica y operativa de la ciberdefensa peruana en el mediano plazo. Este análisis es imperativo para identificar las brechas existentes en la arquitectura de defensa actual y proponer una hoja de ruta que permita al CCFFAA transitar hacia un modelo proactivo, autónomo y altamente resiliente frente a los desafíos que definirá la década venidera.

METODOLOGÍA

El presente trabajo se fundamenta en un diseño de revisión narrativa, cuya naturaleza es simultáneamente descriptiva y prospectiva. Este enfoque permite no solo sintetizar el estado del arte sobre la ciberdefensa en el ámbito militar, sino también proyectar las implicancias de la transformación digital para el Comando Conjunto de las Fuerzas Armadas (CCFFAA) del Perú en el horizonte 2030. La revisión narrativa resulta idónea para abordar temáticas complejas y multidimensionales donde la literatura es dispersa y requiere una interpretación cualitativa de las dinámicas de poder tecnológico, tal como sugieren Green et al. (2006) respecto a la utilidad de estas revisiones para integrar diversos tipos de evidencias en campos en rápida evolución.

La estrategia de búsqueda se estructuró mediante un muestreo intencional de literatura académica, documentos oficiales de defensa y normativas de ciberseguridad. Para asegurar el rigor, se consultaron repositorios de instituciones clave como el Ministerio de Defensa del Perú, la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, y manuales de doctrina militar. Asimismo, se incorporaron reportes de organismos internacionales, incluyendo la Organización de los Estados Americanos (OEA) y el Centro de Excelencia en Ciberdefensa Cooperativa de la OTAN (CCDCOE), cuya literatura es indispensable para contrastar las mejores prácticas globales con las realidades regionales (CCDCOE, 2023).

La temporalidad del estudio abarca fuentes publicadas entre 2020 y 2026. Este marco cronológico es estratégico, dado que permite capturar la aceleración digital post-pandemia y la respuesta institucional ante las amenazas híbridas emergentes. La proyección al 2030 se sostiene mediante un análisis de tendencia que utiliza los datos recopilados para modelar posibles escenarios operativos bajo los actuales planes de desarrollo nacional (PCM, 2021).

La estrategia de análisis se basa en una síntesis crítica y comparativa. Se empleó un procedimiento de triangulación de datos donde los objetivos estratégicos nacionales se cruzaron con las capacidades tecnológicas identificadas en la literatura técnica. Este proceso permite identificar tres dimensiones fundamentales: a) las tendencias de digitalización en el mando y control (C4I); b) las brechas críticas de capacidad, especialmente en cuanto a la formación de capital humano y soberanía de software; y c) los factores de riesgo inherentes a la gobernanza de la ciberdefensa militar (Kuehl, 2009). Para organizar el análisis, se adoptó una lógica de "escenarios de amenazas", lo cual facilita la discusión sobre la resiliencia sistémica en lugar de la defensa estática. Esta metodología garantiza que las conclusiones no sean meramente especulativas, sino derivaciones lógicas de la convergencia entre la doctrina vigente y las proyecciones tecnológicas actuales, permitiendo establecer recomendaciones sólidas para la planificación estratégica del CCFFAA en el mediano plazo.

RESULTADOS

El proceso de transformación digital dentro del Comando Conjunto de las Fuerzas Armadas (CCFFAA) del Perú se encuentra en una etapa de transición crítica. Actualmente, el diagnóstico de los sistemas de Mando, Control, Comunicaciones y Computación (C4I) revela una infraestructura que, si bien ha avanzado en la digitalización administrativa, aún enfrenta retos significativos en cuanto a la integración de sistemas de combate interconectados. Según el Plan Estratégico de Modernización del Sector Defensa, el desafío principal reside en migrar de una arquitectura fragmentada hacia una red ciber-resiliente que garantice la interoperabilidad real entre las tres fuerzas (Ejército, Marina y Fuerza Aérea), superando los silos tecnológicos que limitan la eficacia operativa (Ministerio de Defensa, 2024).

En relación con la evolución del ciberespacio como dominio militar, la doctrina actual del CCFFAA ha comenzado a reconocer formalmente la ciberdefensa no como un apoyo logístico, sino como una función operativa esencial. Sin embargo, existe una tensión entre la doctrina militar tradicional y las exigencias de agilidad que impone la ciberguerra. La doctrina debe evolucionar para adaptarse al concepto de "defensa activa", donde la capacidad de respuesta debe ser casi instantánea ante incidentes. Como señala Libicki (2021), la naturaleza del ciberespacio exige que las organizaciones de defensa trasciendan la mera protección perimetral para adoptar una postura centrada en la detección temprana y la contención proactiva.

En cuanto a los factores críticos identificados, destacan tres ejes fundamentales. Primero, la automatización mediante inteligencia artificial y análisis de datos se presenta como una necesidad ineludible para procesar el volumen masivo de información en los centros de operaciones. Segundo, la protección de la infraestructura crítica nacional (ICN) se ha convertido en una responsabilidad estratégica, dado que los ataques a servicios como energía, telecomunicaciones y transporte afectan directamente la estabilidad nacional (Choucri, 2018). Tercero, la brecha de capital humano es quizás el factor más limitante; el CCFFAA requiere un modelo de retención de talento altamente especializado, capaz de competir con las demandas del sector privado, que a menudo ofrece mejores condiciones para los especialistas en ciberseguridad.

Las proyecciones para el periodo 2026-2030 sugieren dos escenarios posibles. Un escenario optimista implica una inversión sostenida en soberanía tecnológica, donde el Perú desarrolla herramientas de ciberdefensa propias, logrando una madurez operativa que permite la gestión autónoma de incidentes complejos. Por el contrario, un escenario de inversión insuficiente mantendría al país en una posición reactiva, con una dependencia crítica de tecnologías de terceros y una vulnerabilidad persistente frente a amenazas híbridas. La madurez operativa al 2030 dependerá, en gran medida, de la velocidad con la que se institucionalice el talento ciber-especializado y se logre la convergencia tecnológica en el sistema C4I nacional (Singer & Friedman, 2014).

DISCUSIÓN

La transformación digital del Comando Conjunto de las Fuerzas Armadas (CCFFAA) no puede entenderse como un proceso aislado, sino como un esfuerzo de integración intersectorial. La ciberdefensa nacional exige una arquitectura de colaboración público-privada robusta, donde el intercambio de información sobre ciberamenazas entre el Estado, la academia y las empresas tecnológicas privadas sea fluido y constante. En este sentido, la cooperación intersectorial es vital para identificar vulnerabilidades antes de que sean explotadas, transformando la defensa en un activo compartido de seguridad nacional (Kuehl, 2009). La experiencia comparada sugiere que la falta de articulación entre los actores nacionales genera silos de información que debilitan la postura defensiva frente a adversarios coordinados.

Simultáneamente, surgen desafíos éticos y legales complejos. El uso de herramientas digitales, tanto defensivas como aquellas con capacidades ofensivas, debe alinearse

estrictamente con el Derecho Internacional Público. La ambigüedad en la atribución de ciberataques y la proporcionalidad en la respuesta militar en el ciberespacio continúan siendo temas críticos. Como señalan los principios recogidos en el Manual de Tallin, las operaciones militares en el ciberespacio deben regirse por las mismas normas de distinción y proporcionalidad que rigen el conflicto armado tradicional, lo cual requiere que el Perú fortalezca su marco jurídico interno para regular el accionar del CCFFAA en este dominio (CCDCOE, 2023).

Un componente central en esta discusión es la soberanía tecnológica. La dependencia histórica de proveedores extranjeros para el desarrollo del ecosistema C4I expone al país a riesgos de "puertas traseras" y vulnerabilidades en la cadena de suministro. La transición hacia el 2030 debe priorizar el desarrollo de capacidades locales y la adopción de software soberano, al menos en las capas críticas de la infraestructura de defensa. Según Singer y Friedman (2014), la dependencia de hardware y software desarrollado fuera de las fronteras nacionales es una vulnerabilidad estratégica que debe gestionarse mediante una política de diversificación de proveedores y el fomento de una industria local de ciberseguridad.

Finalmente, la gestión del riesgo debe evolucionar radicalmente. La digitalización expande exponencialmente la superficie de ataque, haciendo obsoletos los modelos de defensa perimetral tradicionales que se basan en el concepto de una "red interna segura". En su lugar, el CCFFAA debe adoptar un modelo de resiliencia sistémica, basado en la arquitectura Zero Trust (confianza cero), donde se asume que la red ya ha sido comprometida y se prioriza la capacidad de detección, contención y recuperación rápida. Como indica Libicki (2021), la resiliencia no busca impedir todo incidente —lo cual es imposible en un entorno interconectado— sino asegurar que la misión principal de las Fuerzas Armadas pueda continuar operando a pesar de las interrupciones digitales. En conclusión, el éxito de la transformación digital peruana reside en equilibrar la agilidad tecnológica con una doctrina de seguridad que entienda la vulnerabilidad no como una excepción, sino como una constante del dominio ciberespacial.

CONCLUSIÓN

La transformación digital del Comando Conjunto de las Fuerzas Armadas (CCFFAA) representa un hito que trasciende la simple modernización técnica; constituye una

profunda metamorfosis cultural y doctrinal. La adopción de tecnologías avanzadas exige que el personal militar internalice el ciberespacio como un dominio de operaciones constante, donde la proactividad y la adaptabilidad son los nuevos pilares de la eficacia institucional.

El periodo 2026-2030 se perfila como un ciclo determinante para la seguridad nacional. Durante esta etapa, el Perú tiene la oportunidad de consolidar un sistema de ciberdefensa autónomo, diseñado para enfrentar con éxito las amenazas híbridas que ya desafían la estabilidad del Estado. Alcanzar este nivel de madurez operativa no es opcional, sino una condición indispensable para garantizar la soberanía en un entorno geopolítico cada vez más digitalizado y volátil.

Para alcanzar estos objetivos, se recomienda enfocar los esfuerzos institucionales en tres ejes estratégicos. Primero, la inversión sostenida en la formación, captación y retención de ciber-talento humano, reconociendo que el capital intelectual es el activo de defensa más crítico. Segundo, el fortalecimiento de la cooperación estratégica intersectorial, integrando al sector privado y a la academia bajo una visión unificada de resiliencia nacional. Finalmente, resulta imperativo establecer mecanismos de actualización continua de protocolos frente a tecnologías disruptivas, como la inteligencia artificial y la computación cuántica. Solo a través de este enfoque multidimensional, el CCFFAA podrá transitar hacia una arquitectura de defensa robusta, resiliente y capaz de salvaguardar los intereses vitales de la nación ante los complejos desafíos de la próxima década.

REFERENCIAS

- CCDCOE. (2023). *Tallinn Manual 3.0: International Law Applicable to Cyber Operations*. Cambridge University Press. <https://ccdcoe.org/research/tallinn-manual/>
- Choucri, N. (2018). *Cyberpolitics in international relations*. MIT Press. <https://doi.org/10.7551/mitpress/10844.001.0001>
- Green, B. N., Johnson, C. D., & Adams, A. (2006). Writing narrative literature reviews for peer-reviewed journals: Secrets of the trade. *Journal of Chiropractic Medicine*, 5(3), 101–117. [https://doi.org/10.1016/S0899-3467\(07\)60142-6](https://doi.org/10.1016/S0899-3467(07)60142-6)

- Kuehl, D. T. (2009). *From cyberspace to cyberpower: Defining key terms*. In F. D. Kramer, S. H. Starr, & L. K. Wentz (Eds.), *Cyberpower and National Security* (pp. 24–42). Potomac Books.
- Libicki, M. C. (2021). *Cyberspace in military operations*. Georgetown University Press. <https://press.georgetown.edu/book/georgetown/cyberspace-military-operations>
- Ministerio de Defensa del Perú. (2024). *Informe anual sobre el estado de modernización del sector defensa*. Oficina de Planeamiento Estratégico. <https://www.gob.pe/mindef>
- Nye, J. S. (2020). *Cyber power and national security*. In *Cyberpower and National Security*. Potomac Books.
- Presidencia del Consejo de Ministros [PCM]. (2021). *Política Nacional de Transformación Digital al 2030*. Gobierno del Perú. <https://www.gob.pe/institucion/pcm/colecciones/403-politica-nacional-de-transformacion-digital>
- Rid, T. (2013). *Cyber war will not take place*. Oxford University Press. <https://doi.org/10.1093/acprof:oso/9780199330416.001.0001>
- Secretaría de Gobierno y Transformación Digital. (2021). *Política Nacional de Transformación Digital al 2030*. Presidencia del Consejo de Ministros del Perú. <https://www.gob.pe/institucion/pcm/normas-legales/1799757-118-2021-pcm>
- Singer, P. W., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press. <https://doi.org/10.1093/wentk/9780199918119.001.0001>
- Tikk-Ringas, E. (2022). *The state of cyber defense: Trends in national security architectures*. Geneva Centre for Security Policy. <https://www.gcsp.ch/publications/the-state-of-cyber-defence>
- Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power in the international system*. Oxford University Press. <https://doi.org/10.1093/oso/9780190844288.001.0001>