Este artículo examina el papel fundamental de la ciberseguridad y la ciberdefensa en el contexto del accionar conjunto moderno. En un entorno digital cada vez más complejo, las Fuerzas Armadas deben desarrollar capacidades robustas que permitan proteger sus infraestructuras críticas, garantizar la continuidad operativa y mantener la superioridad estratégica. A partir de la experiencia del autor en la Maestría en Ciberseguridad y Ciberdefensa del CAEN, se exploran conceptos clave, desafíos emergentes y la necesidad de una cultura "ciberestratégica" integrada en el pensamiento militar actual.

Ciberseguridad y ciberdefensa:
pilares estratégicos para las operaciones conjuntas en el siglo XXI

Cybersecurity and Cyber Defense: Strategic Pillars for Joint Operations in the 21st Century

This article examines the fundamental role of cybersecurity and cyberdefense in the context of modern joint military operations. In an increasingly complex digital environment, Armed Forces must develop robust capabilities to protect critical infrastructures, ensure operational continuity, and maintain strategic superiority. Based on the author's experience in the Master's Degree in Cybersecurity and Cyberdefense at CAEN, key concepts, emerging challenges, and the need for a cyberstrategic culture integrated into current military thinking are explored.

Capitán de Fragata
José Carlo Montoya Ruibal

Licenciado en Ciencias Marítimas Navales por la Escuela Naval del Perú. Primer puesto en la Maestría en Gestión Naviera de la Escuela Nacional de Marina Mercante y el primer puesto del XIX Programa de Comando y Estado Mayor Conjunto (PCEMC) de la Escuela Superior Conjunta de las Fuerzas Armadas. Ha sido distinguido con la Condecoración de las Naciones Unidas por su desempeño en la Misión de Paz en la República Centroafricana (MINUSCA); con la Medalla y el Diploma de Honor al Mérito del Comando Conjunto de las Fuerzas Armadas del Perú por el primer puesto del XIX PCEMC; y con la Navy and Marine Corps Commendation Medal, otorgada por el Department of the Navy de los Estados Unidos, por su desempeño excepcional como Oficial de Enlace. Actualmente se desempeña como Agregado Naval Adjunto a la Embajada del Perú en los Estados Unidos de América y Oficial de Enlace en el Componente Naval del Comando Sur y de la Cuarta Flota de la U.S. Navy.

Montoya, J. (2025). Ciberseguridad y ciberdefensa: pilares estratégicos para las operaciones conjuntas en el siglo XXI. Revista *Pensamiento Conjunto,* Año 13, N° 2. pp. 69-73. ISSN° 2707-367X

Fecha de recepción: 22 de julio de 2025.
Fecha de aceptación: 11 de septiembre de 2025.
Fecha de publicación: 31 de diciembre de 2025.

La transformación digital ha ampliado el campo de batalla hacia el ciberespacio, donde los ataques pueden generar efectos físicos, políticos y estratégicos. En este dominio, la ciberseguridad y la ciberdefensa son ya componentes esenciales del poder nacional y del accionar conjunto. Para el Perú, fortalecer capacidades cibernéticas implica proteger infraestructuras críticas, garantizar continuidad operativa y asegurar la interoperabilidad entre instituciones militares y civiles. Este artículo sintetiza conceptos clave, desafíos emergentes y líneas de acción para consolidar una cultura "ciberestratégica" en operaciones conjuntas, con énfasis en necesidades y realidades del país.

EL CIBERESPACIO COMO NUEVO TEATRO DE OPERACIONES

El ciberespacio es un dominio operacional estratégico donde se disputan ventajas geopolíticas, se vulneran sistemas críticos y se ejecutan operaciones encubiertas. Las amenazas provienen de actores estatales y no estatales (crimen organizado, grupos ideológicos y automatismos hostiles). Proteger mando y control, cadenas logísticas y plataformas conectadas exige una arquitectura de ciberseguridad robusta y adaptable, con doctrina, protocolos y capacidades específicas integradas al pensamiento conjunto.

GESTIÓN DEL RIESGO Y RESILIENCIA EN OPERACIONES MILITARES

La ciberdefensa moderna se centra en gestionar riesgos: anticipar vulnerabilidades, mitigar impactos y recuperar funciones esenciales rápidamente. El NIST Cybersecurity Framework 2.0 ordena estas capacidades en cinco fun-

PALABRAS CLAVE: CIBERSEGURIDAD, CIBERDEFENSA, CIBERESPACIO, INTEROPERABILIDAD, OPERACIONES CONJUNTAS, CIBERCOMANDO, LIDERAZGO DIGITAL, RESILIENCIA OPERACIONAL.
KEYWORDS: CYBERSECURITY, CYBER DEFENSE, INTEROPERABILITY, JOINT OPERATIONS, CYBER COMMAND, DIGITAL LEADERSHIP, OPERATIONAL RESILIENCE.

ciones: identificar (activos, riesgos y dependencias), proteger (controles preventivos), detectar (anomalías e incidentes), responder (contención y erradicación) y recuperar (restauración y mejora continua).

La resiliencia operacional —capacidad de mantener la misión bajo ataque— debe incorporarse al planeamiento desde el nivel táctico hasta el estratégico. Para ello, mediante formación continua, ejercicios realistas y liderazgo con entendimiento técnico-operacional.

CIBERDEFENSA CONJUNTA: UNA NECESIDAD ESTRATÉGICA

La naturaleza transfronteriza y asimétrica de las amenazas cibernéticas obliga a una respuesta coordinada entre Fuerzas Armadas y entidades civiles. Una ciberdefensa conjunta efectiva comparte inteligencia, estandariza protocolos y eleva la disuasión.

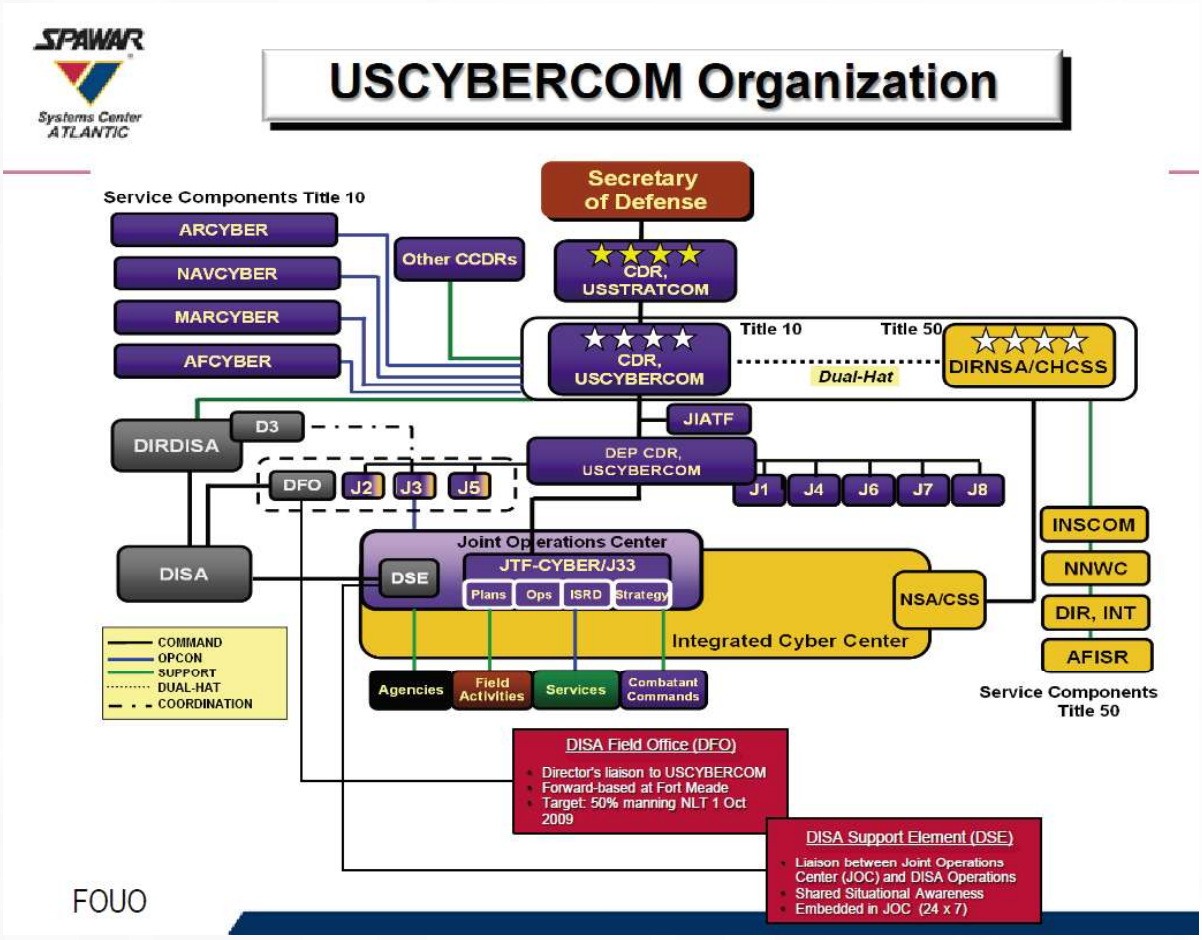
Para el Perú, esto requiere doctrina ciberconjunta articulada por el Comando Conjunto, interoperabilidad técnica (estándares, identidades y redes seguras), procedimientos comunes y plataformas de colaboración confiables con socios nacionales e internacionales.

IMPLEMENTACIÓN DE LA INTEROPERABILIDAD CIBERCONJUNTA

1) Gobernanza: crear un marco de roles y responsabilidades (RACI) entre Comando Conjunto, institutos armados y entidades civiles.

2) Doctrina y normas: aprobar manuales y eglas de

ORGANIGRAMA DEL US CIBERCOMANDO CONJUNTO



Enfrentamiento (ROE) cibernéticas cibernéticas; alinear con NIST CSF 2.0 e ISO/IEC 27001.

3) Capacidades: SOC/CSIRT conjunto; capacidades de ciberinteligencia, threat hunting y respuesta a incidentes.

4) Interoperabilidad técnica: gestión de identidades federadas, segmentación de redes, Zero Trust, cifrado extremo a extremo.

5) Entrenamiento y ejercicios: wargames cibernéticos, ejercicios conjuntos con evaluación independiente (red teaming).

6) Legal y cooperación: protocolos de intercambio de información y coordinación con PCM/SGTD, reguladores y sector privado.

7) Métricas y mejora: indicadores de tiempo de detección, contención y recuperación; lecciones aprendidas y retroalimentación.

CICLO NIST CSF 2.0 (IDENTIFICAR–PROTEGER–DETECTAR–RESPONDER–RECUPERAR).

Fuente: National Institute of Standards and Technology.

CIBERCOMANDO Y LIDERAZGO DIGITAL

Un Cibercomando Conjunto centraliza vigilancia, coordinación y respuesta ante incidentes; impulsa la formación especializada y sostiene una postura de ciberdisuasión.

El liderazgo digital exige visión estratégica, toma de decisiones bajo incertidumbre y dirección de equipos multidisciplinarios. Debe integrar ciberinteligencia (obtención y análisis de información en el ciberespacio), análisis forense, operaciones de información y guerra cognitiva (influir en percepciones y decisiones del adversario).

RETOS Y OPORTUNIDADES EN LA CIBERDEFENSA DEL PERÚ

Retos:
- madurez desigual en infraestructuras críticas;
- brechas de talento y rotación;
- dependencia tecnológica externa;
- coordinación interinstitucional perfectible;
- restricciones presupuestales y marcos legales en evolución.

Oportunidades:
- formación especializada (CAEN y universidades);
- ejercicios y cooperación internacional;
- ecosistema privado-tecnológico local;
- alineamiento con estándares globales.

Líneas de cierre: priorizar riesgos por impacto en misión; fortalecer CSIRT sectoriales; acuerdos de intercambio de inteligencia; compras públicas con requisitos de seguridad; incentivos a I+D y laboratorios de ciberseguridad aplicados a OT/ICS.

EJEMPLOS HISTÓRICOS Y ACTUALES: LECCIONES OPERACIONALES

• Stuxnet (2010): ataque a sistemas industriales (OT). Lección: segmentación estricta IT/OT, control de medios extraíbles y monitoreo de comportamiento en PLC/SCADA.

• NotPetya (2017): malware tipo wiper con vector de cadena de suministro. Lección: seguridad de proveedores y parches; respaldos inmutables.

• Colonial Pipeline (2021): impacto operativo a partir de incidentes IT en una empresa de energía. Lección: planes de continuidad y escenarios cruzados IT/OT, gestión de credenciales y MFA.

• Perú (varios): defacement y ransomware en entidades públicas y gobiernos locales. Lección: higiene básica (parcheo, copias de seguridad, hardening), capacitación y respuesta coordinada con autoridades competentes.

LECCIONES PARA LAS NUEVAS PROMOCIONES

- Ciberconciencia situacional: integrar indicadores de amenazas al planeamiento de misión.
- Interoperabilidad cibernética: procedimientos, lenguaje común y plataformas seguras compartidas.
- Liderazgo ciberestratégico: decisiones basadas en datos, gestión de crisis y comunicación efectiva.
- Entrenamiento continuo: ejercicios conjuntos realistas, red teaming y lecciones aprendidas.
- Resiliencia por diseño: segmentación, Zero Trust, backups verificados y planes de continuidad.

CONCLUSIÓN

La ciberseguridad y la ciberdefensa son ya inseparables del diseño y ejecución de operaciones conjuntas. Para el Perú, asumir el ciberespacio como dominio estratégico implica consolidar doctrina ciberconjunta, interoperabilidad real y liderazgo digital, con métricas y mejora continua. Un Ciber-comando Conjunto, estándares alineados a buenas prácticas internacionales y entrenamiento sostenido permitirán proteger infraestructuras críticas, asegurar la continuidad operativa y fortalecer la disuasión. La misión es clara: operar con seguridad hoy, para asegurar la superioridad y la paz mañana.

REFERENCIAS

Congreso de la República. (2019, 27 de agosto). Ley N.° 30999: Ley de Ciberdefensa [PDF]. Diario Oficial El Peruano / Congreso de la República. https://leyes.congreso.gob.pe/Documentos/2016_2021/ADLP/Texto_Consolidado/30999-TXM.pdf?utm_source=chatgpt.com

Presidencia del Consejo de Ministros [PCM]. (2024, 13 de febrero). Decreto Supremo N.° 017-2024-PCM: Decreto Supremo que aprueba el Reglamento de la Ley N.° 30999, Ley de Ciberdefensa [PDF]. Diario Oficial El Peruano / Gob.pe. Disponible en https://busquedas.elperuano.pe/dispositivo/NL/2261522-1

Presidencia del Consejo de Ministros [PCM]. (2023, 28 de julio). Decreto Supremo N.° 085-2023-PCM: Decreto Supremo que aprueba la Política Nacional de Transformación Digital al 2030 [PDF]. Diario Oficial El Peruano / Gob.pe. https://www.gob.pe/institucion/pcm/normas-legales/4471543-085-2023-pcm

Pascoe, C., Quinn, S. y Scarfone, K. (2024, 26 de febrero). The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Papers, NIST CSWP 29). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.29

Pomerleau, M. (2023, 12 de mayo). New DOD doctrine officially outlines and defines 'expeditionary cyberspace operations'. DefenseScoop. Recuperado de https://defensescoop.com/2023/05/12/new-dod-doctrine-officially-outlines-and-defines-expeditionary-cyberspace-operations/