DOI: 10.59794/rscd.2025.v11i11.149
Sección internacional

Análisis estratégico para la integración del dominio cibernético con los dominios físicos para misiones múltiples de seguridad y defensa
Strategic Analysis for Cyber Domain Integration with Physical Domains for Multiple Security and Defense Missions

Boris Saavedra[1] ORCID: 0009-0000-1334-2833
Chase Logan Boone[2] ORCID: 0009-0002-4356-3260

[1]National Defense University, Venezuela, saavedrab@ndu.edu
[2]National Defense University, Estados Unidos, chase.l.boone.civ@ndu.edu

Autor para correspondencia: Boris Saavedra, saavedrab@ndu.edu

Resumen

La guerra moderna abarca tanto el ámbito físico como el cibernético. Las fuerzas armadas actuales enfrentan amenazas en múltiples dominios, tales como: tierra, mar, aire, espacio y el ciberespacio. Por ello, integrar las operaciones cibernéticas con las operaciones en los dominios físicos se ha vuelto esencial para lograr ventajas en el campo de batalla. La doctrina estadounidense de Operaciones Multidominio (OMD) plantea contrarrestar amenazas simultáneas en todos los dominios de la guerra mediante la convergencia de efectos y fuerzas. Sin embargo, muchos países aliados aún enfrentan desafíos para incorporar plenamente las capacidades cibernéticas a sus operaciones convencionales. Este artículo analiza la importancia de integrar el dominio cibernético con los dominios físicos en las operaciones de seguridad y defensa, apoyándose en la doctrina de Operaciones Multidominio (OMD) de EE. UU., estudios de caso regionales y tendencias hemisféricas, con el fin de orientar a los países de América Latina y el Caribe en la construcción de capacidades multimisión frente a amenazas híbridas.

Palabras clave: Dominio, operaciones multidominio (OMD), guerra cibernética,

sistemas ciberfísicos (SCF), inteligencia artificial generativa (IAG)

Abstract

Modern warfare encompasses both the physical and cybernetic realms. Today's armed forces face threats in multiple domains, such as land, sea, air, space, and cyberspace. As such, integrating cyber operations with operations in the physical domains has become essential to achieving advantages on the battlefield. The U.S. doctrine of Multi-Domain Operations (MDO) proposes countering simultaneous threats in all domains of warfare through the convergence of effects and forces. However, many allied countries still face challenges in fully incorporating cyber capabilities into their conventional operations. This article analyzes the importance of integrating the cyber domain with the physical domains in security and defense operations, based on the U.S. Multi-Domain Operations (MDO) doctrine, regional case studies, and hemispheric trends, in order to guide Latin American and Caribbean countries in building multi-mission capabilities against hybrid threats.

Keywords: Domain, Multi-Domain Operations (OMD), Cyber Warfare, Cyber-Physical Systems (SCF), Generative Artificial Intelligence (IAG)

Recibido: 03/ 04/ 2025
Revisado: 21/ 08/ 2025
Aprobado: 25/ 09 / 2025

1. Introducción

En la era de la guerra cibernética y la IAG, las principales potencias y otros Estados han aumentado sus arsenales con capacidades cibernéticas cuya utilidad se deriva en gran medida de su opacidad y negabilidad, y en algunos casos, de su actuación en los ambiguos límites de la desinformación, la recopilación de inteligencia, el sabotaje y el conflicto tradicional, creando estrategias sin doctrina reconocida. Sin embargo, cada avance ha ido acompañado de vulnerabilidades (Kissinger, Schmidt & Huttenlocher,

2021). En el contexto de la defensa y la seguridad, un dominio se refiere a una esfera o medio especifico en el que se llevan a cabo actividades militares o de seguridad para alcanzar objetivos este concepto es fundamental para la estrategia militar moderna, en particular en el marco de las operaciones multidominio.

El mundo de tecnologías digitales emergentes, aceleradas y convergentes actual, el concepto de seguridad ha evolucionado para abarcar no solo las amenazas digitales, sino también las vulnerabilidades físicas. Esta convergencia de la seguridad digital y física se materializa con la aparición de los sistemas SCF. Comprender sus complejidades es crucial para la integración del dominio cibernético con los dominios físicos.

La protección de nuestra sociedad cada vez es más compleja y vulnerable. En esencia, sistema ciberfísico consta de tres elementos esenciales: infraestructura física, infraestructura informática y redes de comunicaciones que facilitan la integración de procesos informáticos y físicos que combinan sensores, actuadores y comunicación en red para monitorizar y controlar entidades físicas. Esta fusión fluida de los dominios digitales y físicos permite la creación de sistemas inteligentes e interconectados que pueden interactuar fluidamente con el mundo físico (Blue Goat Cyber, 2025).

En los dominios físicos los sistemas de armas representan los elementos tangibles como armas, barcos de guerra y aviones de combate que funcionan en forma inteligente por estar equipados con sensores que recopilan datos sobre su entorno y actuadores que les permiten interactuar en el mundo físico. El dominio cibernético abarca los componentes de software y hardware que permiten el procesamiento y análisis de datos y comunicaciones.

La creciente complejidad de las operaciones modernas de seguridad y defensa ha exigido una transición hacia una seguridad integrada en múltiples dominios operativos. El concepto de misiones multidominios se centra en la sincronización de las iniciativas de ciberseguridad en entornos aéreos, terrestres, marítimos, espaciales y cibernéticos. Con el auge de las amenazas híbridas, los ataques ciberfísicos y la guerra electrónica, las organizaciones de defensa deben adoptar un enfoque holístico de la defensa que garantice la interoperabilidad fluida, el intercambio de inteligencia y la mitigación de amenazas (Verma, 2025).

El ataque de Estados Unidos a las instalaciones nucleares iraníes, conocido como Operación Martillo de Medianoche, ocurrido el 22 de junio, a las 2:15 a.m. hora de Irán se desarrolló bajo la doctrina de Operaciones Multidominio (OMD) las fuerzas

armadas de los Estados Unidos plantean que el éxito en los conflictos actuales y futuros depende de la integración estrecha de todos los dominios, incluyendo el ciberespacio y el espectro electromagnético. Esta convergencia exige superar la tradicional separación entre operaciones físicas y cibernéticas, adoptando estructuras organizativas y conceptuales que permitan acciones coordinadas en tiempo real a través de distintos entornos operativos (Perkins, 2018).

La integración de las capacidades cibernéticas con los dominios físicos tradicionales (aire, tierra, mar, espacio) se ha vuelto crucial para los sistemas de defensa modernos, ya que los adversarios explotan cada vez más las vulnerabilidades en la intersección de la infraestructura digital y física. Este artículo tiene como objetivo hacer un análisis estratégico para examinar la convergencia de la seguridad y defensa ciberfísica, sus desafíos y las soluciones emergentes para la resiliencia de misiones multidominio con una perspectiva hemisférica.

En este contexto, los conflictos modernos evidencian que ninguna misión de seguridad o defensa puede ignorar la dimensión cibernética: los ataques informáticos pueden paralizar infraestructuras críticas, socavar la confianza pública y extender los efectos de un conflicto más allá del campo de batalla tradicional El dominio cibernético abarca los componentes de software y hardware que permiten el procesamiento y análisis de datos, así como las capacidades de ataque y defensa en el ámbito digital (Vergara Cobos & Diao, 2024).

El concepto de seguridad ha evolucionado para abarcar no solo las amenazas digitales, sino también las vulnerabilidades físicas, dando lugar a la convergencia ciber-física. Esta se materializa con los sistemas SCF, que combinan infraestructura física, infraestructura informática y redes de comunicación para controlar entidades físicas mediante sensores y actuadores. La integración fluida entre lo digital y lo físico permite la creación de sistemas inteligentes e interconectados con aplicaciones militares estratégicas. En los dominios físicos, los sistemas de armas modernos están cada vez más equipados con sensores y capacidades de inteligencia artificial que dependen de la robustez de su integración con redes cibernéticas seguras.

La creciente complejidad de las operaciones de defensa exige una transición hacia una seguridad multidominio. Esta se basa en la sincronización entre dominios terrestre, marítimo, aéreo, espacial y cibernético para garantizar interoperabilidad, intercambio de inteligencia y respuestas efectivas ante amenazas híbridas. La integración de las capacidades cibernéticas con los dominios físicos tradicionales se ha vuelto esencial,

ya que los adversarios explotan cada vez más las vulnerabilidades en la intersección entre infraestructuras digitales y físicas.

En América Latina y el Caribe (ALC), la rápida digitalización ha incrementado la exposición a Ciberamenazas, pero la mayoría de los países aún no ha consolidado capacidades cibernéticas robustas ni logrado una integración efectiva con sus estructuras de defensa física. La región ha experimentado un rápido aumento de incidentes cibernéticos —con una tasa anual de crecimiento del 25% en la última década— al mismo tiempo que exhibe rezagos significativos en sus niveles de protección (Vergara Cobos & Diao, 2024).

Esta combinación convierte al ciberespacio en un frente atractivo para actores maliciosos, como cibercriminales, grupos insurgentes, organizaciones criminales transnacionales o incluso Estados que emplean medios híbridos. Casos recientes, como el ciberataque masivo de ransomware contra Costa Rica en 2022 – que llevó a declarar un estado de emergencia nacional sin precedente – demuestran que las agresiones digitales pueden traducirse en crisis de seguridad nacional con impacto tangible en la economía, la gobernanza y la confianza institucional (Collier, 2022).

2. Desarrollo

El Ejército de EE. UU. adopta nueva doctrina de operaciones multidominio

Las doctrinas militares de EE. UU. ofrecen una base para integrar eficazmente la dimensión cibernética. Manuales y publicaciones conjuntas del Ejército reconocen al ciberespacio como un dominio operativo más. El concepto de Multi Domain Operations (OMD), según el manual del 1 de octubre de 2022, busca integrar todos los dominios (tierra, mar, aire, espacio y ciberespacio) para enfrentar adversarios pares. Esta integración combina ciberataques, guerra electrónica, información, fuego convencional y maniobra física. Unidades especializadas como los ‘Multi-Domain Task Forces’ ejemplifican esta visión. Estos batallones integran inteligencia de señales, espacio y ciberespacio para apoyar a fuerzas convencionales. El objetivo: generar efectos coordinados y multiplicar el poder en tiempo real.

Sin embargo, las doctrinas por sí solas no ganan batallas. Persisten desafíos en interoperabilidad tecnológica, estructura de mando, y formación de personal. Muchos ejércitos aliados carecen de una estructura organizativa que vincule estrechamente a los comandantes de operaciones cibernéticas con los comandantes de fuerzas terrestres, aéreas, navales o espaciales. Del mismo modo, la capacitación tradicional suele aislar la seguridad cibernética en unidades de IT, en lugar de entrenar a todos los niveles en escenarios donde lo cibernético y lo físico convergen. Este desfase doctrinal y organizativo puede llevar a demoras en la respuesta ante ciberamenazas durante combates convencionales, o a una falta de comprensión y comunicación mutua entre expertos técnicos y comandantes tácticos (Feickert, 2024).

3. Situación actual del dominio cibernético en américa latina y el caribe

América Latina y el Caribe enfrentan una encrucijada en ciberseguridad. La digitalización ha generado sociedades interconectadas, pero la capacidad institucional no ha crecido al mismo ritmo. Informes destacan que ALC es la región con mayor crecimiento en incidentes cibernéticos divulgados, con un aumento anual del 25% en la última década. A la vez, es una de las menos preparadas: según el Índice Global de Ciberseguridad de la Unión Internacional de Telecomunicaciones, su puntaje promedio en ciberseguridad es 10.2 de 20. Esta brecha ha convertido al ciberespacio regional en un "campo de batalla", explotado por actores maliciosos. Las vulnerabilidades técnicas e institucionales son el blanco principal (Vergara Cobos & Diao, 2024).

Los ciberataques en ALC no solo aumentan en número, sino que son más disruptivos y con fines más amplios que el lucro financiero. Un 59% tienen motivaciones políticas, lo que refleja una transición hacia amenazas híbridas con fines de desestabilización. Ejemplos recientes lo demuestran: en 2022, Costa Rica sufrió un ataque con ransomware que generó pérdidas del 2,4% del PIB; en Ecuador y Argentina, filtraciones masivas expusieron datos sensibles; en Chile, un ataque con malware cerró temporalmente un banco estatal; y en 2023, un ataque impidió el voto

en el extranjero en Ecuador. Estas agresiones digitales generan impactos físicos graves (Vergara Cobos & Diao, 2024).

Pese al panorama crítico, la respuesta institucional en ALC ha sido desigual. Algunos países, como Chile, Colombia, Costa Rica, República Dominicana, México, Panamá y Perú, ya cuentan con Estrategias Nacionales de Ciberseguridad activas, lo que permite coordinación y asignación de recursos. Otros, como Bolivia, El Salvador y Honduras, carecen aún de estrategias integrales o están en fase de elaboración. Esto refleja una baja prioridad política en seguridad digital. Además, la región enfrenta escasez de talento especializado e inversión en infraestructura, lo que limita su capacidad de respuesta (Ciberlatam, 2024).

En 2024, la República Dominicana fue elegida para presidir el Grupo de Trabajo sobre Medidas de Fomento de la Confianza en el Ciberespacio (CBMs) de la OEA, consolidándose como uno de los pocos países caribeños con liderazgo hemisférico en ciberseguridad. Además, su CSIRT-RD, miembro del Forum of Incident Response and Security Teams (FIRST) desde 2020, ha fortalecido su integración en la comunidad internacional de respuesta a incidentes, lo que le permite acceder a apoyo técnico y participar activamente en el desarrollo de normativas globales sobre estabilidad en el ciberespacio (Presidencia de la Republica Dominicana, 2024a).

En esencia, el dominio cibernético en ALC se caracteriza actualmente por alto riesgo y preparación dispar. La creciente conectividad y digitalización amplían la superficie de ataque y atraen tanto a ciberdelincuentes oportunistas como a actores más sofisticados (incluyendo grupos auspiciados por Estados) que emplean tácticas híbridas. Si bien los gobiernos han comenzado a reaccionar mediante estrategias, leyes y mayor cooperación, persiste la necesidad de fortalecer integralmente las capacidades cibernéticas nacionales. Este fortalecimiento abarca no solo la dimensión técnica, sino también el desarrollo doctrinal, la capacitación de recursos humanos, la sensibilización política sobre el tema y la integración del ciberespacio dentro del planteamiento general de defensa y seguridad.

4. Conceptualización del dominio cibernético y estructura integradora

En el ámbito militar, el término dominio se refiere a un entorno o ámbito —físico o virtual— en el que se llevan a cabo operaciones y sobre el cual se busca ejercer cierto grado de control o superioridad. Tradicionalmente, las Fuerzas Armadas han reconocido dominios de la guerra como la tierra, el mar, el aire e, incluso desde fines del siglo XX, el espacio ultraterrestre. Desde inicios del siglo XXI, el ciberespacio ha sido ampliamente aceptado como un quinto dominio de las operaciones militares, con características propias pero complementarias a las de los dominios físicos (Pelcastre, 2019; Perkins, 2018). En Latinoamérica y el Caribe, numerosos países se han alineado con esta visión, denominando al ciberespacio como un dominio operacional comparable a los tradicionales . Por ejemplo, doctrinas militares regionales emplean ya el término dominio cibernético o espacio ciber para enmarcar las acciones de defensa y seguridad en entornos digitales (Saavedra, 2019).

Definir conceptualmente el dominio cibernético es esencial para delimitar su alcance y articular cómo interactúa con los demás dominios. De acuerdo con la Real Academia Española (2014), dominio es un ámbito, real o imaginario, de una actividad , mientras que ciberespacio se describe como un ámbito virtual creado mediante medios informáticos interconectados. Desde el plano doctrinal, el profesor Daniel T. Kuehl ha ofrecido una definición operativa del ciberespacio, al describirlo como "un entorno operativo que consiste en la red interdependiente de sistemas de información conectados al Internet, incluyendo las infraestructuras informáticas y de telecomunicaciones, así como los datos que allí residen" (Saavedra, 2019). Con esta concepción, el ciberespacio, si bien intangible a simple vista, tiene una base física real (servidores, cables, enrutadores, dispositivos) y produce efectos medibles en el mundo.

El Comando Cibernético de Estados Unidos (USCYBERCOM) define el ciberespacio como un dominio con tres capas: física (infraestructura, hardware, cables, satélites), lógica (protocolos, software, algoritmos) y de ciberpersona (identidades digitales, redes sociales, interacciones humanas) (2018). Esta última, aunque abstracta, es clave porque refleja la actividad humana en línea. Estas capas demuestran que el ciberespacio no es uniforme, sino una red compleja de tecnología y personas. Protegerlo implica acciones diferenciadas: asegurar la infraestructura, optimizar los sistemas lógicos (ciberdefensa, actualizaciones, detección de intrusos) y gestionar la información e influencia digital (contrarrestar desinformación, proteger datos, educar

usuarios).

Un elemento clave al conceptualizar un dominio es definir qué implica ejercer superioridad en él. En los ámbitos físicos, esto significa emplearlo libremente para operaciones propias mientras se restringe su uso al enemigo. En el dominio cibernético, este concepto se complica por su carácter difuso y la presencia de actores estatales y no estatales. Aun así, puede hablarse de superioridad cibernética como la capacidad de proteger redes propias y mantener la posibilidad de generar efectos ofensivos en el ciberespacio. Esto exige adaptar principios clásicos de la guerra —como sorpresa, seguridad, unidad de comando— al entorno digital, mediante ataques difíciles de atribuir y defensas sólidas (Saavedra, 2018).

Una consideración doctrinal clave es el rol del sector privado en el dominio cibernético. A diferencia de otros dominios controlados por el Estado (como el espacio aéreo o las fronteras), en el ciberespacio más del 90 % de la infraestructura y servicios depende de actores privados. Por tanto, ninguna estrategia de defensa cibernética puede excluir la cooperación público-privada. Militares y agencias deben trabajar con proveedores de Internet, empresas tecnológicas, de telecomunicaciones y del sector financiero para compartir información, definir estándares y coordinar respuestas. En América Latina, esta colaboración se ha formalizado mediante centros nacionales de ciberseguridad o equipos CERT/CSIRT con participación conjunta.

El dominio cibernético puede entenderse doctrinalmente como un entorno operativo multidimensional (físico, lógico y humano) donde se libran acciones de guerra y seguridad. Su control exige capacidades especializadas y la adaptación de principios militares tradicionales. Esta comprensión estructural es esencial para integrarlo con los dominios físicos. Solo entendiendo su alcance, funcionamiento interno y desafíos —como el rol del sector privado, la atribución de ataques o la velocidad de innovación— se pueden diseñar estrategias efectivas. Los casos de Costa Rica, República Dominicana y Colombia muestran cómo algunos gobiernos de la región ya integran el ciberespacio en sus estructuras de seguridad ante amenazas que superan lo físico.

5. Integración de dominios en misiones multidominio - iniciativas actuales

El concepto de Operaciones Multidominio (OMD), originado en la doctrina militar estadounidense, postula que las fuerzas conjuntas deben ser capaces de integrar capacidades en todos los dominios de forma coordinada para alcanzar la superioridad sobre adversarios cada vez más versátiles (Perkins, 2018). En la práctica, esto significa que una misión de defensa o seguridad no se circunscribe a un solo entorno (por ejemplo, terrestre), sino que involucra simultáneamente acciones terrestres, aéreas, navales, espaciales y cibernéticas, todas sincronizadas hacia el mismo objetivo operacional. Lograr tal convergencia requiere no solo cambios doctrinales, sino también innovaciones tecnológicas, entrenamientos conjuntos y nuevas estructuras de mando que permitan la comunicación fluida entre unidades de distintos dominios.

A nivel global, varias iniciativas actuales ejemplifican esfuerzos por materializar las operaciones multidominio. En Estados Unidos, las Fuerzas Armadas han implementado programas experimentales como Project Convergence (del Ejército) y Exercises Red Flag (Fuerza Aérea y Espacial) que integran sensores, plataformas de armas y redes de mando y control en escenarios simulados donde intervienen todos los dominios. La esencia es acortar el ciclo de decisión: que datos recolectados por satélites o ciberinteligencia alimenten en segundos decisiones de maniobra en tierra o ataques de precisión desde el aire, por ejemplo. Esto se soporta en la iniciativa de JADC2 (Joint All-Domain Command and Control), un sistema unificado de mando que conecta a todas las ramas militares en un solo tejido de información. Tales desarrollos están todavía en fases de prueba, pero han arrojado resultados prometedores en ejercicios contra amenazas convencionales y híbridas.

En América Latina, varios países avanzan hacia la integración multidominio en seguridad y defensa. Destaca el Ejercicio Conjunto Multidominio de Ciberdefensa y Guerra Electrónica (denominado Ejercicio “Beato Carlo Acutis I”), realizado por Argentina en 2022. Por primera vez, sus Fuerzas Armadas simularon un ataque combinado —sabotaje de cables submarinos y ciberataques a redes terrestres— para interrumpir la conectividad del país. La respuesta integró navíos como el ARA Piedrabuena, tropas terrestres, defensa aérea con sistemas RBS 70 y equipos de ciberdefensa y guerra electrónica. El objetivo fue sincronizar fuerzas convencionales y capacidades cibernéticas, actualizar procedimientos y extraer lecciones doctrinarias. Participaron más de 400 efectivos y múltiples plataformas aéreas, marítimas y terrestres (Mary, 2022).

Otro ejemplo relevante es la integración entre ciberdefensa y defensa aeroespacial en

el ejercicio multinacional CRUZEX 2024, liderado por Brasil. Tradicionalmente enfocado en operaciones aéreas combinadas, esta edición incorporó por primera vez el componente CRUZEX Cyber, una simulación tipo "Captura la Bandera" (CTF) para entrenar en protección y ataque de sistemas virtuales de apoyo aeroespacial. Participaron más de 3.500 militares de 16 países en escenarios de conflicto regional, promoviendo interoperabilidad y actualización táctica entre fuerzas aéreas. La inclusión de capacidades cibernéticas, aeroespaciales y antiaéreas apuntó a reforzar la preparación operativa en entornos multidominio (Santos, 2024).

Más allá de ejercicios, también hay iniciativas en doctrina y educación para la integración multidominio. Varios países latinoamericanos han actualizado sus documentos doctrinarios conjuntos para incluir explícitamente el concepto de Operaciones Multidominio. Por ejemplo, fuerzas armadas de Chile y Brasil han estudiado las OMD estadounidenses para adaptarlas a sus realidades, especialmente en escenarios como operaciones de paz donde las amenazas pueden ser híbridas. En la educación militar, seminarios y cursos sobre multidominio empiezan a ofrecerse en academias de guerra de la región, a menudo con cooperación de países de la OTAN o el Comando Sur de EE. UU.

En materia de mando, algunos países han establecido comandos conjuntos para integrar dominios. Colombia creó el Comando Conjunto Cibernético (CCOC), que coordina ciberdefensa entre Ejército, Armada y Fuerza Aérea, permitiendo operar el ciberespacio como dominio estratégico junto a otras fuerzas estatales (Villanueva Mendes, 2015). Brasil fundó en 2016 el Comando de Defensa Cibernética (CD Ciber), integrado por sus tres fuerzas, con la misión de proteger infraestructuras críticas y coordinar defensa cibernética. Durante los Juegos Olímpicos de Río 2016, el CD Ciber apoyó la seguridad digital. Desde entonces, ha ampliado su alcance y colabora con la ABIN, consolidando un modelo de integración entre inteligencia y ciberdefensa (EpEx, 2023).

Aunque los avances en ciberdefensa en América Latina varían, comparten un objetivo común: preparar fuerzas que operen integradas en todos los dominios. Ejercicios con componentes cibernéticos, reformas doctrinales y comandos especializados marcan una ruptura con las estructuras tradicionales. A medida que se acumulan experiencias —y se observan conflictos híbridos en otras regiones—, estos esfuerzos probablemente se expandan. La interoperabilidad multidominio no es solo una mejora táctica; es una necesidad estratégica frente a amenazas difusas donde lo civil y lo

militar, lo legal y lo ilícito, se entrecruzan.

6. Estudios de caso: Costa Rica, República Dominicana y Colombia

Para ilustrar la realidad latinoamericana en la integración del dominio cibernético con los dominios físicos, se presentan a continuación tres casos nacionales. Cada caso refleja distintos niveles de desarrollo institucional, diferentes experiencias frente a amenazas cibernéticas y aproximaciones particulares para incorporar el ciberespacio en las misiones de seguridad y defensa.

6.1. Costa Rica: Respuesta nacional a una crisis cibernética sin Fuerzas Armadas

Costa Rica, un país sin ejército desde 1949, delega su seguridad nacional en cuerpos civiles y policiales. Sin embargo, en 2022, enfrentó una de las amenazas cibernéticas más graves del hemisferio cuando el grupo Conti lanzó ataques simultáneos contra casi 30 instituciones públicas, incluyendo ministerios clave como Hacienda y Ciencia y Tecnología, así como empresas estatales de servicios (Revista Summa, 2024). Ante la negativa a pagar rescate, se filtraron datos sensibles, lo que llevó al presidente Rodrigo Chaves a declarar estado de emergencia nacional—la primera vez que el país activaba ese mecanismo por una amenaza digital (Collier, 2022). Hubo interrupciones de servicios, parálisis fiscal y semanas de incertidumbre mientras el gobierno, con apoyo internacional, intentaba contener la crisis.

La respuesta de Costa Rica evidenció tanto las debilidades como la resiliencia institucional de un país sin fuerzas armadas ante un ciberataque de gran escala. En ausencia de un comando militar de ciberdefensa, la gestión de la crisis recayó en el Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT-CR) nacional, y en el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) con el respaldo de cooperación internacional, incluyendo asistencia técnica de Estados Unidos. Se activaron protocolos de contingencia para mantener operativos servicios

esenciales, se aislaron redes comprometidas y se fortaleció el monitoreo de infraestructura crítica, con especial énfasis en la protección de la red eléctrica y las telecomunicaciones para evitar efectos en cascada (Revista Summa, 2024).

Después de contener la crisis inmediata, Costa Rica dio pasos decisivos para fortalecer su ciberseguridad. Se aceleró la implementación de su Estrategia Nacional de Ciberseguridad 2017–2021, hasta entonces rezagada, y se iniciaron planes para una nueva estrategia a largo plazo. En 2023, el país lanzó oficialmente la Estrategia Nacional de Ciberseguridad 2023–2027, lo que marcó un giro hacia una planificación más sostenida. Para 2024, analistas locales destacaban avances notables: mayor presupuesto, autenticación multifactorial en sistemas gubernamentales y ejercicios regulares de simulación de ciberataques. Costa Rica también buscó apoyo internacional, uniéndose a iniciativas del Banco Mundial y foros hemisféricos de ciberresiliencia (Revista Summa, 2024).

El caso de Costa Rica demuestra que, incluso sin fuerzas armadas, un Estado puede (y debe) integrar el dominio cibernético en su estrategia de seguridad nacional, movilizando agencias civiles, fuerzas policiales e inteligencia en torno a un objetivo común. La convergencia ciber-física aquí se refleja en cómo un ataque digital afectó severamente funciones físicas del Estado (recaudación fiscal, atención de salud, etc.), y cómo la respuesta involucró tanto medidas técnicas en redes como acciones legales, diplomáticas y de seguridad pública. Para los países latinoamericanos, Costa Rica sirve de ejemplo de la importancia de prepararse ante Ciberamenazas sistémicas: contar con planes de contingencia, claridad en la cadena de mando (¿quién lidera en caso de ciber crisis?) y alianzas internacionales puede marcar la diferencia cuando la infraestructura digital de la nación está bajo asedio.

6.2. República Dominicana: Construcción de ciberresiliencia y liderazgo regional

La República Dominicana ha emergido como un actor clave en la ciberseguridad del Caribe, desarrollando una arquitectura institucional sólida y participando activamente en foros internacionales. Aunque posee Fuerzas Armadas, ha delegado la gestión del

ciberespacio en entidades civiles, reconociendo la necesidad de coordinación público-privada. En 2018, adoptó su primera Estrategia Nacional de Ciberseguridad (2018–2021), y en 2022 aprobó la Estrategia Nacional de Ciberseguridad 2030, que orienta su visión a largo plazo. El Centro Nacional de Ciberseguridad (CNCS), bajo el Ministerio de la Presidencia, coordina acciones, supervisa la estrategia y responde ante incidentes (Ciberlatam, 2023).

Un hito importante fue la emisión del Decreto 685-22 de Ciberseguridad en 2022, que estableció obligaciones concretas para las instituciones de la administración pública en materia de protección cibernética . Este decreto institucionaliza la notificación obligatoria de incidentes: todos los organismos públicos deben reportar eventuales ciberataques o brechas de seguridad al CNCS y al CSIRT sectorial correspondiente en un plazo máximo de 24 horas . Asimismo, fija principios y lineamientos para elevar la madurez de ciberseguridad en el sector público, exige la adopción de estándares internacionales, la gestión proactiva de riesgos y la compartición de información sobre amenazas . En efecto, la República Dominicana está construyendo una cultura de ciberseguridad gubernamental, con reglas claras y canales formales de coordinación, lo que redunda en mayor integración del dominio cibernético en las operaciones cotidianas del Estado (Ciberlatam, 2023).

Aunque la República Dominicana no ha enfrentado un ataque tan disruptivo como el de Costa Rica, sí ha gestionado incidentes significativos. Entre 2021 y 2022, el CNCS reportó cerca de 980 eventos en instituciones del Estado, contenidos sin consecuencias graves gracias al trabajo del CSIRT-RD y al monitoreo activo de redes (Presidencia de la República Dominicana, 2023). Además, se registraron más de 4 mil millones de intentos de ciberataques, lo que confirma la presión constante sobre la infraestructura digital pública. En 2023, el gobierno lanzó un sistema de alerta automática de vulnerabilidades para instituciones públicas, fortaleciendo la capacidad preventiva del país (Presidencia de la República Dominicana, 2025).

En el frente militar, si bien la ciberdefensa en la República Dominicana es liderada por entidades civiles como el Centro Nacional de Ciberseguridad (CNCS), las Fuerzas Armadas han comenzado a integrar el componente cibernético en su planificación estratégica. Según el ministro de Defensa, teniente general Carlos Antonio Fernández Onofre, la modernización militar desde 2022 ha incluido inversiones significativas en tecnología, inteligencia y mejoras en los controles para fortalecer la ciberseguridad institucional, como parte de un plan amplio de fortalecimiento del aparato militar

nacional (Villegas, 2025).

La Estrategia Nacional de Ciberseguridad 2030 (2022), establecida por el Decreto 313-22, reconoce la dimensión de defensa cibernética como un componente estratégico, con responsabilidades compartidas entre el Ministerio de Defensa, el Departamento Nacional de Investigaciones (DNI), y otras agencias relevantes. La estrategia enfatiza la protección de infraestructuras críticas y la prevención del ciberterrorismo mediante políticas coordinadas, capacitación especializada y la integración de estándares internacionales. Estas acciones se complementan con el liderazgo del Centro Nacional de Ciberseguridad (CNCS), que supervisa la implementación general y fomenta la colaboración público-privada para fortalecer la ciberresiliencia nacional.

Además, el presidente Luis Abinader anunció en 2022 una histórica inversión en defensa, que incluyó la adquisición de helicópteros, aeronaves de vigilancia, vehículos blindados, y la instalación de una valla fronteriza inteligente con Haití equipada con sensores, cámaras y drones militares. Aunque no se detalla públicamente, la ciberseguridad de estos sistemas de vigilancia fronteriza presumiblemente forma parte de los esfuerzos integrales para proteger las capacidades tecnológicas del Estado (HaitiLibre, 2022).

Un rasgo distintivo del caso dominicano es su liderazgo regional e internacional en temas ciber. Además de participar en el grupo de la OEA mencionado, la República Dominicana ha sido sede de reuniones hemisféricas de equipos CSIRT (en agosto de 2024 organizó la primera reunión de trabajo para desarrollar un protocolo regional de asistencia inmediata ante crisis cibernéticas) (Presidencia de la Republica Dominicana, 2024b). Tal liderazgo tiene beneficios tangibles: ante un incidente grave, la República Dominicana puede recurrir con facilidad a sus contrapartes internacionales para recibir apoyo técnico; del mismo modo, su voz tiene peso en la discusión de normativas globales sobre estabilidad en el ciberespacio.

La experiencia dominicana demuestra que, incluso con recursos limitados, un país de ingresos medios puede integrar el dominio cibernético en su arquitectura de seguridad si hay voluntad política y una estrategia clara. La Estrategia 2030, el CNCS y normativas como el Decreto 685-22 han establecido un marco institucional exigente. Su proyección internacional revela una comprensión madura del ciberespacio como un entorno interdependiente, donde la cooperación es clave. Para países con condiciones similares, este enfoque resalta la importancia de institucionalizar buenas

prácticas, como el reporte de incidentes, y asumir un rol activo en la comunidad internacional de ciberseguridad.

6.3. Colombia: Militarización del ciberespacio y combate a amenazas híbridas

Colombia, con un extenso historial de desafíos de seguridad internos (conflicto con guerrillas, narcotráfico, crimen organizado), ha reconocido tempranamente el ciberespacio como un frente más de confrontación contra amenazas tanto estatales como no estatales. A diferencia de Costa Rica o República Dominicana, Colombia ha militarizado en buena medida la gestión del dominio cibernético, creando estructuras dedicadas de ciberdefensa en el seno de sus Fuerzas Militares y articulándolas con sus estrategias de seguridad nacional. Este enfoque se explica, en parte, porque el país ha sufrido no solo ataques cibernéticos del tipo convencional (fraudes financieros, ransomware, etc.) sino también campañas de ciberterrorismo y desinformación vinculadas con actores armados ilegales y con injerencias externas en su panorama de conflicto interno (Pelcastre, 2019).

El pilar de la integración ciber-física colombiana es el Comando Conjunto Cibernético (CCOC) de las Fuerzas Militares, creado oficialmente a inicios de la década de 2010 como primera línea de defensa en el quinto dominio. Su misión es planear y conducir operaciones militares en el ciberespacio para contrarrestar amenazas a la seguridad nacional, desde la protección de redes institucionales hasta el análisis forense digital y la implementación de protocolos de defensa informática (Cruz Rubio, 2021).

Si bien no se han documentado públicamente operaciones ofensivas contra infraestructuras específicas de grupos armados, documentos doctrinales confirman que las capacidades del CCOC incluyen operaciones ofensivas diseñadas para interrumpir, degradar o destruir redes informáticas y sistemas del adversario cuando sea necesario. Estas acciones buscan afectar el normal funcionamiento de las operaciones enemigas, como parte integral del poder militar en el ciberespacio . En contextos de operaciones especiales, incluso se plantea la incorporación táctica de

agentes cibernéticos para insertar código malicioso en redes hostiles, lo que permite neutralizar o interrumpir comunicaciones críticas bajo presión operativa (Cruz Segura & Di Genaro, 2024).

Además, el CCOC monitorea redes sociales y espacios digitales para detectar campañas de desinformación o propaganda destinadas a socavar la estabilidad del Estado. Este enfoque responde a la comprensión de que las guerras modernas se libran también con narrativas e influencia sobre la opinión pública . Las operaciones cibernéticas de Colombia, tal como lo definen documentos institucionales, abarcan todo el ciclo de prevención, vigilancia, neutralización y recuperación en caso de incidentes, con un énfasis especial en proteger la infraestructura crítica nacional que sustenta servicios esenciales como energía, salud, telecomunicaciones y defensa (Cruz Segura & Di Genaro, 2024).

Operativamente, el Comando Conjunto Cibernético (CCOC) colombiano se ha dotado de capacidades especializadas en ciberdefensa, incluyendo plataformas tecnológicas, personal entrenado, y coordinación con entidades como colCERT y el Centro Cibernético Policial. Entre sus funciones está proveer ciberinteligencia, proteger infraestructuras críticas y liderar la respuesta ante incidentes que comprometan la seguridad nacional (Mora Gámez, & Baquero, 2022, pp. 125-139). Durante las protestas sociales de 2021, grupos hacktivistas como Anonymous vulneraron sitios gubernamentales clave; la respuesta técnica para mitigar estos ataques involucró al ecosistema de ciberdefensa del país, incluyendo al CCOC en colaboración con otras entidades como ColCERT y CCP (Mora Gámez, & Baquero, p. 127).

Los resultados de esta estrategia se observan en varios planos. Colombia ha logrado frustrar ciberataques significativos y mitigar su impacto. Entre 2017 y 2019, el país registró más de 53.000 incidentes de seguridad informática atribuidos a crimen organizado transnacional (principalmente robo de dinero e identidad) , pero gracias a una postura proactiva ("mantener nunca la defensa abajo" en palabras de un oficial) , no se han materializado daños catastróficos en infraestructuras críticas (Pelcastre, 2019).

En respuesta a la ofensiva del ELN en la región del Catatumbo a inicios de 2025, el Ejército colombiano desplegó 300 soldados con apoyo de la Fuerza Aeroespacial para neutralizar los enfrentamientos con disidencias de las FARC y proteger a la población civil, incluyendo la evacuación de heridos y la asistencia a familias desplazadas (Xinhua Español, 2025). Estas operaciones ofensivas también buscaron controlar

corredores de movilidad clave y restablecer la seguridad en centros urbanos como Tibú, epicentro de una de las crisis humanitarias más graves desde el acuerdo de paz de 2016 (SWI, 2025).

En términos normativos, Colombia también ha avanzado: su documento de política CONPES 3701 de 2011 ya delineaba la necesidad de integrar ciberseguridad y ciberdefensa, y fue actualizándose con una Política de Seguridad Digital 2020–2022. Actualmente, se discute en el Congreso el proyecto de ley 023 de 2023 que crearía la Agencia Nacional de Seguridad Digital, con el objetivo de coordinar y centralizar funciones dispersas entre el Ministerio de Defensa, la Policía Nacional, la Fiscalía y otros actores institucionales, optimizando la respuesta del Estado ante incidentes cibernéticos (Mejía Marulanda, 2024). De lograrse, esta agencia civil se complementaría con el Comando Conjunto Cibernético ya existente, fortaleciendo el ecosistema nacional de ciberseguridad.

En conclusión, Colombia ofrece un ejemplo de integración ciber-física como parte de una estrategia de defensa nacional consolidada. El país ha desarrollado capacidades multimisión en el dominio cibernético, usándolas tanto para proteger sus infraestructuras y redes gubernamentales como para apoyar operaciones contra amenazas tradicionales (guerrilla, terrorismo, crimen organizado). Al tratar al ciberespacio como otro frente de su prolongado conflicto interno, Colombia ha innovado en tácticas conjuntas, combinando acciones cinéticas con operaciones en línea. La experiencia colombiana ofrece lecciones útiles para países que enfrentan amenazas híbridas, al subrayar el valor de contar con unidades especializadas, fusionar inteligencia digital y convencional, y adaptar la doctrina militar a la realidad del conflicto virtual.

7. Capacidades multimisión ante amenazas híbridas - recomendaciones y casos destacados

Las amenazas híbridas son un desafío cada vez más común en la seguridad global y regional, caracterizado por la combinación de métodos convencionales e irregulares con fines estratégicos. El concepto alude a la articulación de capacidades regulares e

irregulares —acciones militares abiertas junto con tácticas encubiertas o no militares— dirigidas a un mismo objetivo (Fernández Córdoba, 2024). En lugar de un enfrentamiento directo, los actores hostiles (estatales o no) explotan vulnerabilidades en varios dominios: lanzan ciberataques, fomentan disturbios, difunden propaganda, emplean proxis para sabotaje y recurren al crimen organizado o al terrorismo. El resultado es un entorno difuso, donde la línea entre guerra y paz se desdibuja y las instituciones deben responder en varios frentes a la vez.

Frente a estas amenazas híbridas, las naciones necesitan desarrollar capacidades multimisión, entendidas como la aptitud de sus fuerzas de seguridad y defensa para cumplir misiones diversas y simultáneas en diferentes dominios. A continuación, se presentan recomendaciones estratégicas para fortalecer dichas capacidades en el contexto latinoamericano, acompañadas de ejemplos de países que están encabezando esfuerzos en cada aspecto:

1. Adoptar un enfoque integral de seguridad nacional. Las estructuras estatales deben evitar divisiones estrictas entre seguridad interna (a cargo de policías) y defensa externa (a cargo de militares) cuando enfrentan amenazas híbridas, ya que estas desdibujan dicha frontera. Se recomienda establecer marcos de coordinación inter agencial permanentes (ej. comités nacionales de seguridad cibernética e híbrida) que integren a militares, policías, inteligencia civil, autoridades regulatorias y sector privado. Por ejemplo, Colombia ha integrado sus esfuerzos contra la desinformación combinando recursos de inteligencia militar (CCOC) con su Centro Cibernético Policial, logrando respuestas unificadas a campañas de influencia malignas .
2. Fortalecer la ciberdefensa como componente central de la defensa nacional. Más allá de la inversión en tecnología, esto requiere contar con equipos de respuesta rápida, analistas en inteligencia de señales, hackers éticos y un marco legal claro que defina las reglas de operación en el ciberespacio. Estados Unidos y las naciones de la OTAN han establecido Ciber comandos con mandato tanto defensivo como ofensivo, que en los últimos conflictos (por ejemplo, frente a amenazas rusas) han realizado operaciones de “caza hacia adelante” desarticulando malware antes de que ataque sus redes (Pomerleau, 2025). En América Latina, Brasil con su Comando de Defensa Cibernética, ha invertido en simuladores y ejercicios internacionales (como los mencionados CRUZEX Cyber) para preparar a su personal. Cada país debería considerar la creación o el fortalecimiento de comandos conjuntos de ciberdefensa, con una línea directa al más alto nivel militar para asegurar su peso en la planificación

estratégica.

3. Desarrollar fuerzas flexibles y versátiles. Las amenazas híbridas pueden exigir, por ejemplo, que en una misma misión humanitaria las tropas deban lidiar con desinformación en redes locales, protegerse de drones comerciales armados y mantener redes de comunicación seguras frente a hackeos. Para ello, es necesario que las unidades militares y policiales sean versátiles o cuenten con destacamentos especializados integrados. Una buena práctica la ofrece Francia con su concepto de "GTIA aéroterrestre" usado en operaciones en África, donde cada Grupo Táctico incluye no solo infantería y blindados, sino especialistas en guerra electrónica e inteligencia de señales para contrarrestar los artefactos explosivos improvisados detonados vía celular por terroristas. Trasladado a Latinoamérica, cuando las fuerzas mexicanas o centroamericanas enfrentan carteles de la droga (que a veces emplean tácticas híbridas con corrupción de información, comunicaciones cifradas, etc.), deberían desplegar ya con equipos de ciberinteligencia y guerra electrónica que intercepten y bloqueen las comunicaciones enemigas. Argentina, con el ejercicio en Las Toninas, ya probó la eficacia de combinar tropas convencionales con expertos de ciber/electrónica en un solo operativo . La recomendación es institucionalizar estas unidades conjuntas multidominio a nivel táctico, para que se entrenen juntas de antemano y tengan procedimientos estandarizados.

4. Aumentar la cooperación internacional y regional. Ningún país puede abordar solo amenazas que, por naturaleza, atraviesan fronteras (virus informáticos globales, campañas de desinformación que ignoran límites geográficos, redes criminales transnacionales). Es crucial aprovechar marcos multilaterales. La OEA ya trabaja en confianza cibernética, pero podría expandir sus ejercicios de simulación híbrida. Mediante su Programa de Ciberseguridad y la resolución CICTE/RES.1/17, la OAE ha promovido medidas de cooperación técnica entre sus Estados miembros. También existen centros de excelencia como el Centro Europeo de Excelencia contra Amenazas Híbridas (COE en Finlandia), con el cual países americanos pueden colaborar para intercambiar lecciones aprendidas de escenarios en Europa del Este. Estados Unidos ha potenciado la asistencia en ciberseguridad a sus aliados latinoamericanos a través del Comando Sur (USSOUTHCOM), mediante acuerdos de cooperación, ejercicios conjuntos y revisiones técnicas en países como Costa Rica, Paraguay, Panamá, El Salvador y Argentina (Hamilton & Ruiz, 2023; Thomas, 2022; U.S. Southern Command, 2024). Esta colaboración incluye actividades como el

fortalecimiento de centros de operaciones cibernéticas, intercambios de expertos en defensa cibernética con Argentina, y ejercicios como CENTAM Guardian, donde equipos de ciberdefensa de Guatemala, El Salvador y Honduras practicarán en redes simuladas (Nelson, 2022; Thomas, 2022). Asimismo, espacios regionales como la conferencia CENTSEC han incorporado temas de ciberseguridad en sus agendas, consolidándose como foros clave para enfrentar amenazas emergentes y fortalecer capacidades compartidas (Pelcastre, 2025). Se recomienda formalizar alianzas regionales enfocadas en amenazas híbridas, que complementen los mecanismos de defensa existentes e integren actores civiles—como un Task Force hemisférico contra la desinformación electoral.

5. Invertir en inteligencia estratégica y anticipación. Las amenazas híbridas suelen gestarse silenciosamente antes de desencadenarse abiertamente. Un Estado debe poder detectar signos tempranos en múltiples dominios: rumores en la Deep web de un ataque inminente, movimientos financieros inusuales, agrupación de fuerzas paramilitares, campañas mediáticas sospechosas. Esto requiere una inteligencia fusionada que combine fuentes tradicionales (humanas, señal, geoespaciales) con ciberinteligencia e inteligencia artificial para analizar grandes datos. En América Latina, un caso emergente es Chile, que en su reciente Política Nacional de Ciberseguridad 2023–2028 priorizó el fortalecimiento de la infraestructura institucional y técnica, incluyendo la creación de una Agencia Nacional de Ciberseguridad (ANCI), aunque sin contemplar aún un centro dedicado exclusivamente al análisis de amenazas híbridas (IMF, 2024; Biblioteca del Congreso Nacional del Chile, 2023). Se recomienda a los países destinar parte de sus fondos de seguridad y defensa a herramientas analíticas avanzadas (por ejemplo, sistemas de Big Data para redes sociales que alerten sobre campañas coordinadas) y entrenar analistas con mentalidad "híbrida" capaces de correlacionar eventos dispersos.

6. Fortalecer la resiliencia societal y la comunicación estratégica. Las amenazas híbridas apuntan a explotar fracturas dentro de la sociedad objetivo (divisiones políticas, desconfianza en instituciones) y provocar reacciones desproporcionadas. Por ello, la respuesta no es solo militar/policial, sino que involucra la resiliencia de la población y una hábil gestión de la información por parte del gobierno. Programas educativos de ciber higiene, alfabetización mediática para reconocer noticias falsas, protocolos para continuidad de negocios en sector privado, son parte de las capacidades multimisión menos tangibles pero cruciales. Varios países europeos han

implementado conceptos de “defensa total” que involucran a la ciudadanía en la protección del país (por ej., Finlandia y Estonia, muy conscientes de la amenaza híbrida rusa, donde cada ciudadano tiene un rol en resiliencia). En Latinoamérica, se podría emular en contextos locales: Costa Rica, tras su ataque de 2022, ha fomentado fuertemente la cultura de la ciberseguridad en sector público y privado , mientras Colombia ha desplegado campañas para fortalecer la confianza en la Fuerza Pública ante la propaganda hostil. La recomendación es elaborar planes nacionales de resiliencia híbrida, que incluyan desde respaldos energéticos para cortes de luz intencionales, hasta manuales de comportamiento ciudadano ante campañas de miedo o caos fomentadas artificialmente.

En cuanto a países que destacan en el desarrollo de capacidades multimisión contra amenazas híbridas en el hemisferio occidental, además de los casos ya mencionados de Colombia, Brasil, República Dominicana y Argentina, cabe resaltar a Estados Unidos y Canadá como referentes por sus avanzadas doctrinas y recursos. Estados Unidos, mediante su concepto de Deterrence by Denial en ciberespacio y la implementación de fuerzas de tarea multidominio en unidades del Ejército, está marcando pautas que aliados cercanos como Colombia buscan seguir (Lane, 2023). Canadá, a través de su enfoque de seguridad nacional integral (incluyendo protección de procesos electorales contra injerencia extranjera y un centro de ciberseguridad puntero), ofrece un modelo adaptado a un país con población y extensión moderada, similar a muchos latinoamericanos.

En el contexto latinoamericano, México empieza a dar señales de abordar amenazas híbridas ligadas al crimen organizado al integrar inteligencia financiera, ciberinteligencia e incursiones armadas de manera más sincronizada contra cárteles. Perú y Ecuador, tras experiencias de crisis política acompañadas de ciberataques (por ejemplo, los ataques del grupo Guacamaya que expusieron miles de documentos militares en 2022), están reestructurando sus sistemas de inteligencia y ciberdefensa para no ser sorprendidos de nuevo. En suma, la región en su conjunto se halla en distintas etapas, pero la tendencia es clara: las capacidades multimisión dejarán de ser una opción deseable para convertirse en una necesidad estratégica ineludible ante la realidad de las amenazas híbridas.

8. Imperativos operacionales para la integración

1. Neutralización de Amenazas Híbridas

Los conflictos modernos combinan ciberataques con ataques cinéticos, como el incidente del gusano Stuxnet (que atacó sistemas de control industrial) y las interrupciones en activos militares dependientes del GPS. La integración entre dominios permite respuestas sincronizadas a estas amenazas multivectoriales.

2. Interdependencia de la Infraestructura

Las comunicaciones espaciales, las redes inteligentes y los sistemas de armas autónomos dependen de arquitecturas ciberfísicas interconectadas. Por ejemplo: un BESS (Sistema de Almacenamiento de Energía de Baterías) comprometido podría desestabilizar las redes eléctricas o los sistemas de propulsión naval, lo que podría generar riesgos con efectos en cascada.

3. Interoperabilidad Aliada

Iniciativas como las Operaciones Multidominio de la OTAN y el JADC2 (All-Domain Command and Control) del Departamento de Defensa de EE. UU. hacen hincapié en protocolos estandarizados para el intercambio seguro de datos en los dominios aéreo, terrestre, marítimo, espacial y cibernético.

9. Desafíos claves

Integración de Sistemas diferentes con protocolos incompatibles dificultan la fusión de datos en tiempo real. Esto demanda actualizaciones modulares de las puertas de enlace de las aplicaciones de la interfaz de programación de aplicaciones (API). Vulnerabilidades de la cadena de suministro Los componentes comprometidos (por ejemplo, unidades de BESS (Battery Energy Storage Systems) fabricadas en China tienen una arquitectura de puertas traseras de confianza cero, auditorías de hardware. Ampliación de la superficie de ataque mediante los dispositivos conectados por Internet de las cosas y operaciones tecnológicas. (IoT/OT) en sistemas navales y de aviación crean puntos de entrada. La Segmentación de red, detección de anomalías

mediante el empleo de IAG.

Disyuntiva entre velocidad y seguridad por los retrasos en el cifrado de las comunicaciones en el campo de batalla. El empleo de algoritmos resistentes a la tecnología cuántica y computación muy sofisticada.

10. Recomendaciones estratégicas

1. Estructuras de mando unificadas

Establecer grupos de trabajo ciberfísicos conjuntos (p. ej., la Agencia Cibernética de Defensa de la India) para supervisar las operaciones Inter dominio.

2. Armonización de estándares

Adoptar los marcos de operaciones multidominio por ejemplo en la OTAN para la comunicación cifrada Inter dominio y los manuales de respuesta a incidentes.

3. Fortalecimiento de la cadena de suministro

Exigir certificaciones de componentes de terceros y fabricación local para sistemas críticos como los BMS (sistemas de gestión de baterías).

4. Entrenamiento basado en simulación

Realizar simulacros de guerra que simulen ataques cibernéticos coordinados contra infraestructuras multidominio. La fusión de la ciberseguridad y la seguridad física ya no es opcional, sino un imperativo estratégico. Aprovechar la arquitectura interoperable, la criptografía avanzada y los sistemas de comando potenciados por IAG, las organizaciones de defensa pueden lograr resiliencia ante las amenazas híbridas en constante evolución. El éxito dependerá de romper los silos o situaciones Inter dominio que puedan obstaculizar las comunicaciones entre los equipos de ciberseguridad y seguridad física, como lo demuestran iniciativas de primera línea como JADC2 de los EE. UU y el Comando Espacial Integrado de la India.

11. Conclusiones

Integrar plenamente el dominio cibernético con los dominios físicos es hoy un imperativo estratégico para las fuerzas armadas del siglo XXI. Las operaciones cibernéticas ya no son un complemento, sino un multiplicador de poder que puede inclinar la balanza en conflictos modernos. La sinergia entre acciones cinéticas y digitales permite responder de manera más eficaz ante amenazas híbridas, mientras que su ausencia puede generar vacíos operacionales críticos.

En América Latina y el Caribe, la creciente exposición a Ciberamenazas contrasta con capacidades defensivas aún desiguales. El análisis regional evidencia que los países mejor preparados —como Colombia, República Dominicana o Brasil— han comenzado a consolidar estructuras ciberfísicas integradas, aunque en diferentes etapas de madurez. Estas experiencias demuestran que no existe una fórmula única, pero sí principios comunes: planificación interinstitucional, entrenamiento conjunto, y adopción de doctrinas operativas que incorporen al ciberespacio desde la fase táctica.

Asimismo, la integración de dominios no debe limitarse al ámbito militar. Las amenazas híbridas actuales atacan infraestructura crítica, redes sociales, procesos democráticos y cohesión social. Por ello, las capacidades multimisión deben incluir no solo fuerzas armadas entrenadas en operaciones multidominio, sino también ciudadanía informada, marcos legales modernos y alianzas público-privadas. La defensa efectiva frente a estos retos exige una respuesta convergente, coordinada y adaptada a las realidades del hemisferio.

En resumen, avanzar hacia una convergencia ciber-física no es solo una aspiración técnica, sino una necesidad estratégica para preservar la soberanía, la seguridad y la estabilidad regional. Al adaptar los principios de las Operaciones Multidominio (OMD) a los contextos latinoamericanos, los países del hemisferio podrán fortalecer su interoperabilidad, disuadir agresiones y responder con mayor resiliencia a las complejidades del entorno operativo contemporáneo.

Referencias

Biblioteca del Congreso Nacional de Chile. (2023). *Construyendo la ciberseguridad en Chile.* Comisión Desafíos del Futuro, Ciencia, Tecnología e Innovación. https://www.forociber.cl/foro/site/docs/20240322/20240322150520/edicion_construyendo_la_ciberseguridad_en_chile_v2.pdf

Blue Goat Cyber. (2025). *Cyber-Physical Systems: Bridging Digital and Physical Security [Sistemas ciberfísicos: Tendiendo puentes entre la seguridad digital y la*

física]. https://bluegoatcyber.com

Ciberlatam. (2023). República Dominicana publica el decreto 685-22 de ciberseguridad. *Segurilatam*. https://www.segurilatam.com/actualidad/republica-dominicana-publica-el-decreto-685-22-de-ciberseguridad_20230103.html

Ciberlatam. (2024). Estas son las estrategias nacionales de ciberseguridad de los países latinoamericanos. *Segurilatam*. https://www.segurilatam.com/ciberilatam/estas-son-las-estrategias-nacionales-de-ciberseguridad-de-los-paises-latinoamericanos_20240514.html

Collier, K. (2022, 8 de mayo). Costa Rica declara estado de emergencia ante ataque cibernético masivo estilo ransomware. *NBC News.* https://www.nbcnews.com/tech/tech-news/costa-rica-declares-state-emergency-ransomware-attack-rcna28415

Cruz Rubio, J. (2021). *Defendiendo el ciberespacio: Una aproximación al estado de Colombia frente a la ciberdefensa* [Tesis de maestría, Universidad Militar Nueva Granada]. Repositorio Institucional UMNG. https://repository.umng.edu.co/server/api/core/bitstreams/67dd16a6-dfb8-4244-961e-8cd887469aba/content

Cruz Segura, J. G., & Di Genaro, R. (2024). Soporte cíber a Fuerzas Especiales del Ejército colombiano en ambiente táctico. En L. Montero Moncada & O. A. Garzón Gómez (Eds.), *Comandos: Retos de las Fuerzas Especiales e Inteligencia en la guerra contemporánea* (pp. 163-188). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602809.07

Estrategia Nacional de Ciberseguridad 2022. Gobierno de República Dominicana. https://cncs.gob.do/wp-content/uploads/2022/07/Decreto-313-22.pdf

EpEx. (2023). *Consolidação do Comando de Defesa Cibernética.* Exército Brasileiro. http://www.epex.eb.mil.br/index.php/ultimas-noticias/497-consolidacao-do-comando-de-defesa-cibernetica

Feickert, A. (2024). *Defense primer: Army multi-domain operations (MDO) [Manual de defensa: Operaciones multidominio del Ejército].* Congressional Research Service. https://www.congress.gov/crs_external_products/IF/PDF/IF11409/IF11409.13.pdf

Fernández Córdoba, J. (2024, 4 de febrero). La tecnología multidominio y la amenaza híbrida: el enemigo invisible ya está aquí. *El Confidencial.* https://www.elconfidencial.com/espana/2024-02-04/foro-desafios-defensa-amenaza-híbrida-guerra-multidominio_3823290/

HaitiLibre. (2022, 7 de junio). Haiti - Security: Very important purchases of military equipment in the Dominican Republic [Haití - Seguridad: Compras muy importantes

de material militar en la República Dominicana]. *HaitiLibre.* https://www.haitilibre.com/en/news-37851-haiti-security-very-important-purchases-of-military-equipment-in-the-dominican-rep.html

Hamilton, J., & Ruiz, V. (2023). Employing strategic cyber competition in Latin America [Emplear la cibercompetencia estratégica en América Latina]. *Journal of the Americas,* 5(2), 274-298. https://www.airuniversity.af.edu/Portals/10/JOTA/journals/Volume-5_Issue-2/23-Hamilton-Ruiz_eng-w.pdf

International Monetary Fund. [IMF] (2024). *Cybersecurity and financial stability: Considerations for Chile [Ciberseguridad y estabilidad financiera: Consideraciones para Chile]*. https://www.elibrary.imf.org/view/journals/002/2024/042/article-A002-en.xml

Kissinger, H. A., Schmidt, E., & Huttenlocher, D. (2021). *The age of AI and our human future [La era de la inteligencia artificial y nuestro futuro humano]*. Little Brown.

Lane, G. (2023). Operationalizing deterrence by denial in the cyber domain [Operacionalización de la disuasión por denegación en el ciberespacio]. *Military Cyber Affairs*, 6(1). https://scholarcommons.usf.edu/mca/vol6/iss1/

Mary, G. (2022, 15 de julio). Argentina realiza el primer ejercicio conjunto de ciberdefensa y guerra electrónica. *InfoDefensa.* https://www.infodefensa.com/texto-diario/mostrar/4076957/argentina-realiza-primer-ejercicio-conjunto-multidominio-ciberdefensa-guerra-electronica

Mejía Marulanda, M. (2024, 28 de septiembre). Sin haberse creado la Agencia de Seguridad Digital ya genera polémica: congresistas denuncian posible 'mico'. *Infobae*. https://www.infobae.com/colombia/2024/09/28/sin-haberse-creado-la-agencia-de-seguridad-digital-ya-genera-polemica-congresistas-denuncian-posible-mico/

Mora Gámez, I. H., & Baquero Valdés, F. (2022). Capacidades del Estado colombiano para combatir las amenazas y los desafíos multidimensionales en los dominios aéreo y ciberespacial. En F. Baquero Valdés (Ed.), *Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano* (pp. 109-151). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602106.03

Nelson, V. (2022, 20 de diciembre). NH Guard, Salvadoran cyber teams strengthen partnership [La Guardia Nacional y los equipos cibernéticos salvadoreños refuerzan su colaboración]. *U.S. Southern Command.* https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3258497/nh-guard-salvadoran-cyber-teams-strengthen-partnership/

Pelcastre, J. (2019, 12 de junio). Militares colombianos en guerra contra cibercriminales. *Diálogo Américas.* https://dialogo-americas.com/es/articles/militares-colombianos-en-guerra-contra-cibercriminales/

Pelcastre, J. (2025, 1 de abril). Central America builds on CENTSEC for security [Centroamérica se apoya en CENTSEC para su seguridad]. *Diálogo Américas.* https://dialogo-americas.com/articles/central-america-builds-on-centsec-for-security/

Perkins, D. G. (2018). Preparándonos para combatir hoy: Las operaciones multidominio y el Manual de Campaña 3-0. *Military Review,* (3), 2-12. https://www.armyupress.army.mil/Journals/Edicion-Hispanoamericana/Archivos/Tercer-Trimestre-2018/Preparandonos-para-combatir-hoy/

Pomerleau, M. (2025, 1 de abril). Cybercom discovered Chinese malware in South American nations—Joint Chiefs chairman nominee [El Cibercomando descubrió malware chino en países sudamericanos]. *DefenseScoop.* https://defensescoop.com/2025/04/01/cybercom-chinese-malware-south-america-dan-caine-joint-chiefs-trump/

Presidencia de la República Dominicana. (2023, 7 de noviembre). El Centro Nacional de Ciberseguridad ha atendido alrededor de 980 incidentes cibernéticos en instituciones del Estado. *Ministerio de la Presidencia.* https://minpre.gob.do/comunicacion/notas-de-prensa/el-centro-nacional-de-ciberseguridad-ha-atendido-alrededor-de-980-incidentes-ciberneticos-en-instituciones-del-estado

Presidencia de la República Dominicana. (2024a, 19 de febrero). *República Dominicana lidera el Grupo de Trabajo de Medidas de Fomento de la Confianza en el Ciberespacio de la OEA.* https://presidencia.gob.do/noticias/republica-dominicana-lidera-el-grupo-de-trabajo-de-medidas-de-fomento-de-la-confianza-en

Presidencia de la República Dominicana. (2024b, 9 de mayo). *República Dominicana reúne a líderes de los Equipos de Respuesta ante Incidentes Cibernéticos (CSIRT) nacionales de América Latina y el Caribe*. https://presidencia.gob.do/noticias/republica-dominicana-reune-lideres-de-los-equipos-de-respuesta-ante-incidentes

Presidencia de la República Dominicana. (2025, 3 de abril). *La República Dominicana es sede de evento internacional sobre ciberseguridad y diplomacia cibernética*. https://presidencia.gob.do/noticias/la-republica-dominicana-es-sede-de-evento-internacional-sobre-ciberseguridad-y-diplomacia

Real Academia Española. (2024). *Diccionario de la lengua española* (23.a ed.). https://dle.rae.es/dominio

Revista Summa. (2024, 20 de marzo). ¿Cómo ha avanzado Costa Rica en ciberseguridad tras la ola de ataques del 2022? *Revista Summa.* https://revistasumma.com/como-ha-avanzado-costa-rica-en-ciberseguridad-tras-la-ola-de-ataques-del-2022/

Saavedra, B. (2019, 11 de junio). El papel de los militares en el ciberespacio como dominio: implicancias, retos y oportunidades. *CEEEP*. https://ceeep.mil.pe/2019/06/11/el-papel-de-los-militares-en-el-ciberespacio-como-dominio-implicancias-retos-y-oportunidades/

Santos, E. (2024, 13 de noviembre). Fuerza Aérea Brasileña inicia Ejercicio CRUZEX 2024. *Diálogo Américas.* https://dialogo-americas.com/es/articles/fuerza-aerea-brasilena-inicia-ejercicio-cruzex-2024/

SWI. (2025, 12 de enero). Colombia anuncia inicio de 'operaciones ofensivas' en zona afectada por ataques del ELN. *Swissinfo*. https://www.swissinfo.ch/spa/colombia-anuncia-inicio-de-%22operaciones-ofensivas%22-en-zona-afectada-por-ataques-del-eln/88765163

Thomas, L. (2022, 20 de mayo). U.S. Army South, Argentine army work to strengthen cybersecurity capabilities [El Ejército Sur de EE. UU. y el Ejército argentino trabajan para reforzar capacidades en ciberseguridad]. *U.S. Southern Command.* https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3056987/us-army-south-argentine-army-work-to-strengthen-cybersecurity-capabilities/

U.S. Southern Command. (2024, 11 de marzo). U.S. Strengthens cybersecurity partnership with Paraguay [EE. UU. refuerza su alianza con Paraguay en seguridad cibernética]. https://www.southcom.mil/MEDIA/NEWS-ARTICLES/Article/3979394/us-strengthens-cybersecurity-partnership-with-paraguay/

Vergara Cobos, E., & Diao, H. (2024, 3 de abril). De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo. *Banco Mundial Blogs.* https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe

Verma, D. (2025, 5 de enero). Cross-domain security: Integrating air, land, sea, and space cyber defense [Seguridad entre dominios: Integración de la ciberdefensa aérea, terrestre, marítima y espacial]. *LinkedIn*. https://www.linkedin.com/pulse/cross-domain-security-integrating-air-land-sea-space-cyber-verma-aepcc

Villanueva Mendes, J. C. (2015). *La ciberdefensa en Colombia* [Tesis de maestría, Universidad Piloto de Colombia]. http://polux.unipiloto.edu.co:8080/00002646.pdf

Villegas, L. (2025, 12 de mayo). Military institutional strengthening, pivotal goal of Dominican Defense Minister Onofre [El fortalecimiento institucional militar, objetivo

central del ministro de Defensa dominicano Onofre]. *Diálogo Américas*. https://dialogo-americas.com/articles/military-institutional-strengthening-pivotal-goal-of-dominican-defense-minister-onofre/

Xinhua Español. (2025, 19 de enero). Ejército colombiano refuerza operaciones contra guerrilla ELN tras ataques. *Xinhua*. https://spanish.xinhuanet.com/20250119/87e0c56f2d4149928a3c638979447332/c.html