RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Integración de dominios y ejércitos multimisión: De operaciones conjuntas al multidominio

Integration of Domains and Multi-Mission Armies: from joint to multi-domain operations

Recibido: 01/ 05 / 2025 | Revisado: 15 / 07 / 2025 | Aprobado: 30 / 09 / 2025
DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

Teniente coronel Kelvin Leandro Encarnación González, ERD
República Dominicana

Correo: kelvinencarnacióng@gmail.com

ORCID: https://orcid.org/0009-0004-2488-5090

Afiliación: Universidad Nacional para la Defensa

El autor es teniente coronel del Ejército de la República Dominicana. Es máster en Seguridad, Defensa y Geoestrategia, así como en Derecho y Relaciones Internacionales; posee la Especialidad en Comando y Estado Mayor para Fuerzas Terrestres (graduado de honor, 2021); la Especialidad en Derechos Humanos y Derecho Internacional Humanitario; es licenciado en Derecho (Magna Cum Laude); y licenciado en Ciencias Militares de la Academia Militar de las Fuerzas Armadas "Batalla de las Carreras". Ha realizado, además, un Diplomado Internacional en Operaciones Psicológicas y Psicosociales; un Diplomado en Comunicación Estratégica para la Seguridad y Defensa Nacional; un Diplomado en Ciberdefensa y Ciberseguridad; un Diplomado en Metodología de la Investigación Científica; un Diplomado en el Modelo Educativo UNADE; un Diplomado en Gobernabilidad y Administración de Cooperativas (2023); un Diplomado en Seguridad Fronteriza; un Diplomado en Hacienda e Inversión Pública; un Diplomado en Derecho Procesal Civil; un Diplomado en Derecho de Familia; un Diplomado en Derecho Inmobiliario; un Diplomado en Derecho Laboral y Seguridad Social; y un Diplomado en Derecho de Familia (2009), entre otros cursos y talleres especializados. Durante su carrera ha ocupado numerosas funciones de relevancia, tales como: director de Pensiones de la Junta de Retiro y Fondo de Pensiones de las Fuerzas Armadas; subdirector de Planificación y Desarrollo del Instituto de Seguridad Social de las Fuerzas Armadas; subdirector de Recursos Humanos del mismo instituto; y docente titular de la Escuela de Graduados del Ejército de la República Dominicana (EGEMERD), en asignaturas como Defensa Nacional, Planificación para la Defensa, Fundamentos de Seguridad y Defensa Nacional, entre otras materias militares del bloque de Doctrina del Ejército y Operaciones Conjuntas. A lo largo de casi 26 años de servicio ininterrumpido, ha adquirido capacidades, experiencias y cualidades de liderazgo que le han permitido cumplir de manera efectiva con las misiones asignadas.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

Resumen

En el presente artículo se analiza que en las últimas décadas, tanto la guerra como las operaciones militares han experimentado una mutación considerable. De la coordinación de fuerzas terrestres, aéreas y navales, se ha pasado a un concepto más amplio: las operaciones multidominio. El concepto de operaciones conjuntas se afianzó posterior a la Segunda Guerra Mundial y a lo largo de la Guerra Fría. Para entonces, cualquier fuerza militar que pretendiera alzarse con el éxito debía contar con el apoyo de las demás fuerzas. En 2018, el Comando de Entrenamiento y doctrina del Ejército de los Estados Unidos (TRADOC) publica un concepto doctrinal formal para las Operaciones Multidominio, en donde las define como operaciones en múltiples dominios y espacios disputados para superar las fortalezas de un adversario presentándole múltiples dilemas operativos y tácticos. Las Operaciones Multidominio desvanecen la frontera entre el conflicto, la crisis y la paz, igualmente entre lo convencional y lo no convencional, constituyéndose esto, junto a la disuasión y la escalada, en aspectos estratégicos característicos de este tipo de operaciones. República Dominicana, en cuanto a los medios materiales, enfrenta el reto tecnológico de adoptar las capacidades propias de las operaciones multidominio con recursos un tanto limitados. Las guerras del futuro tienen mucha probabilidad de continuar por el camino de la integración multidominio y añadiéndose más tecnología que revolucionará la forma de combatir; y las fronteras que separan lo humano y la máquina, lo civil y lo militar, será cada vez más difusa.

Palabras clave: Operaciones multidominio, ciberespacio, multimisión, operaciones conjuntas, guerra híbrida

Abstract

In this article, we will examine how, in recent decades, both warfare and military operations have undergone considerable transformation. From the coordination of land, air, and naval forces, we have moved toward a broader concept: multi-domain operations. The concept of joint operations became entrenched after World War II and throughout the Cold War. By then, any military force seeking success had to rely on the support of other forces. In 2018, the United States Army Training and Doctrine Command (TRADOC) published a formal doctrinal concept for Multi-Domain Operations, defining them as operations in multiple domains and contested spaces to overcome an adversary's strengths by presenting them with multiple operational and tactical dilemmas. The Multi-Domain Operations blur the lines between conflict, crisis, and peace, as well as between conventional and unconventional operations. This, along with deterrence and escalation, constitutes characteristic strategic aspects of this type of operation. In terms of material resources, the Dominican Republic faces the technological challenge of adopting the capabilities of multi-domain operations with somewhat limited resources. Wars of the future are likely to continue along the path of multi-domain integration, adding more technology that will revolutionize the way we fight; and the lines separating human and machine, civilian and military will become increasingly blurred.

Keywords: Multi-domain operations, cyberspace, multi-mission, joint operations, hybrid warfare

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

Introducción

La guerra históricamente ha significado el uso de las fuerzas convencionales o no, que, por medio de una organización estructurada de éstas, de forma estratégica y coordinada, tienen como estado final deseado hacerse con un objetivo previamente planteado, a través, de las tradicionalmente conocidas operaciones conjuntas.[1] En décadas recientes, tanto la guerra como las operaciones militares han experimentado una mutación considerable, pues, de la coordinación de las fuerzas terrestres, aéreas y navales, se ha pasado a un concepto más amplio: las operaciones multidominio (MDO, por sus siglas en inglés).

El enfoque e/o integración multidominio reconoce una extensión del campo de batalla moderno, más amplia y extensa de los límites conocidos de los dominios físicos ya conocidos, que ahora incluyen nuevas áreas como el ciberespacio, el espacio ultraterrestre y el ámbito cognitivo o informativo inclusive. La transición de una cooperación entre fuerzas armadas tradicionales hacia las MDO no solo representa un cambio conceptual, sino que conlleva una transformación doctrinal exhaustiva y profunda; por las implicaciones que tiene pasar de la acostumbrada coordinación entre fuerzas (ejércitos, armadas y fuerzas aéreas) a la integración de manera sincronizada de las herramientas militares y no militares disponibles, que van desde misiones en tierra hasta operaciones espaciales, cibernéticas e informativas y/o psicológicas.

Los hechos de las últimas décadas han demostrado que no es suficiente dominar un ámbito de la guerra, sino dominarlos todos a la vez o por lo menos negar al enemigo esa ventaja, creando múltiples dilemas al mismo, con tanta rapidez que este se vea limitado al responder. Atendiendo a lo anterior, pretendemos en este artículo describir cómo ha sido la evolución de las operaciones conjuntas hacia las operaciones multidominio y la integración de éstas. Procuramos analizar el concepto desde el punto de vista histórico y conocer las implicaciones tecnológicas de este tipo de guerra para el nivel estratégico. Además, describiremos casos recientes de cómo y dónde han sido aplicadas estas operaciones.

Finalmente, pretendemos enfocarlo hacia los retos para las Fuerzas Armadas de República Dominicana al momento de adoptar dicho tipo de operación y brevemente exponer las tendencias que a futuro presenta la guerra en múltiples dominios y sus implicaciones a partir de la dirección que proyecta.

1 La manera básica en la que el Departamento de Defensa (DOD) emplea dos o más Servicios (de al menos dos Departamentos Militares) en una única operación es mediante operaciones conjuntas. Las operaciones conjuntas son acciones militares realizadas por las fuerzas conjuntas y las fuerzas del Servicio empleadas en relaciones de mando específicas, pero que no conforman fuerzas conjuntas. Una fuerza conjunta está compuesta por elementos importantes, asignados o agregados, de dos o más Departamentos Militares que operan bajo un único comandante de Fuerza Conjunta o JFC (Publicación Conjunta [JP], 3-0, 2018).

Desarrollo

De Operaciones Conjuntas a Multidomio: Evolución.

A la participación coordinada de más de una rama de las Fuerzas Armadas en una operación se le conoce como operaciones conjuntas. De acuerdo con la publicación conjunta JP 3-0 (2018), la manera básica en la que el Departamento de Defensa (DOD,[2] emplea dos o más Servicios (de al menos dos Departamentos Militares) en una única operación es mediante operaciones conjuntas. Una fuerza de este tipo está compuesta por elementos importantes, asignados o agregados, de dos o más Departamentos Militares que operan bajo un único comandante de la Fuerza Conjunta (JFC).

El concepto de operaciones conjuntas se afianzó a partir de la finalización de la Segunda Guerra Mundial y a lo largo de la Guerra Fría. Para entonces estaba claro que cualquier fuerza militar que pretendiera alzarse con el éxito en combate debía contar con el apoyo de las demás fuerzas. Es por esto por lo que vimos cómo occidente y su doctrina desarrollaron el concepto de armas combinadas[3] con el fin de aprovechar y explotar sus fortalezas complementarias (Manual de campo [FM], 100-5, 1982). Entrada la década de 1980 irrumpe en escena el concepto de Batalla Aeroterrestre introducido por el Ejército de Estados Unidos, que consistía y hacia énfasis en una sincronización armoniosa y total de las fuerzas terrestres y las fuerzas del aire a los fines de alcanzar profundidad en las operaciones y que permitiera la derrota del enemigo de manera eficiente (Manual de campo [FM], 100-5, 1982).

La doctrina descrita anteriormente sienta las bases de "lo conjunto", indicando básicamente, que las unidades y armas serán siempre más efectivas siempre y cuando operen en conjunto, no así si lo hacen de manera individual o por separado ((Manual de campo [FM], 100-5, 1982, pp. 7-3); significando esto la importancia de la integración de fuerzas en las operaciones, obviando por completo la individualización de las acciones. La experiencia de la Guerra del Golfo en 1991 lleva a gran parte de las potencias militares a acoger de manera absoluta las operaciones conjuntas como parte de su doctrina. Los triunfos conseguidos en la operación Tormenta del Desierto demostraron la eficacia de una campaña conjunta (tierra, mar y aire), con el apoyo simultaneo de información satelital y de geolocalización y una robusta y eficaz logística.

Posteriormente, el Departamento de Defensa de los Estados Unidos en su visión conjunta a 2020, aspiraba a obtener la superioridad en todos los ámbitos de la guerra con la implementación del concepto de operaciones del espectro total. No obstante, a inicios del siglo XXI, la aparición de nuevas tecnologías y con esto, de nuevas amenazas, tales como las estrategias anti-acceso/denegación de área (A2/AD), el apogeo del ciberespacio como escenario de conflictos y el espacio ultraterrestre y su militarización, empezaron a exponer las limitaciones de la doctrina conjunta tradicional.

La aparición de estos entornos y la necesidad de enfrentarlos al nivel adecuado hace que las potencias militares empiecen a ser conscientes de enfocar las operaciones militares hacia

2 Equivalente al Ministerio de Defensa para el caso de República Dominicana.
3 Consiste en integrar infantería, blindados, artillería, fuerzas aéreas tácticas, etc., en un esfuerzo unificado.

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

los dominios múltiples. Por medio del impulso dado por el Ejército de Estados Unidos, el concepto de multidominio resalta en la década del 2010, específicamente como operaciones multidominio (MDO por sus siglas en inglés), buscando operar frente a adversarios (El Rusia y China) que claramente podían desafiarlos en varios dominios a la vez. El Comando de Entrenamiento y Doctrina del Ejército de los Estados Unidos (TRADOC) (2018). Pública un concepto doctrinal formal para las Operaciones Multidominio en donde las define como, cito: "operaciones en múltiples dominios y espacios disputados para superar las fortalezas de un adversario presentándole múltiples dilemas operativos y/o tácticos" (p. 6).

Según Borne (2019), lo que procuran las MDO es aprovechar el dominio terrestre, aéreo, marítimo, espacial, ciberespacial y otros como el espectro electromagnético y la información de manera simultánea, para alcanzar efectos complementarios que detengan o anulen la respuesta de un enemigo. Las MDO representan un salto cualitativo, aunque en sus inicios algunos consideraban que era una modificación o extensión de las batallas aeroterrestres de la década de los 80, pues, procura no solo coordinar a fuerzas convencionales, sino que busca integrar de manera efectiva nuevas capacidades, como drones, inteligencia artificial, guerra electrónica (EW), operaciones psicológicas (PSYOPS) y ciberataques.

Como también señalan King y Boykin (2019), las MDO no son unas "Airland Battle 2.0", sino que incluye nuevas herramientas y escenarios que anteriormente se consideraban ajenos a una operación militar tradicional o convencional. Es por esto por lo que el nuevo enfoque que requiere el multidominio procura descentralizar la planificación y la ejecución a los niveles bajos, permitiendo a los comandantes sincronizar efectos en diversos ámbitos en tiempo real,[4] consiguiendo que haya una afinidad en las acciones que sean concebidas desde la planificación, difuminando las fronteras antes estrictas, entre lo terrestre, naval, aéreo, etc., y creando un único espacio interconectado de batalla.

Actualmente, gran parte de las potencias militares del mundo están en el proceso de incorporación del concepto de multidominio en sus doctrinas; siendo los Estados Unidos, según Brading (2021), quienes han procurado acelerar el paso con la implementación de iniciativas que crean Fuerzas de Tarea Multidominio (MDTF por sus siglas en inglés) en su Ejército, y el desarrollo de la estrategia conjunta de Mando y Control Conjunto en todos los Dominios (JADC-Joint All Domain Command and Control) que procura conectar los diferentes nodos y sensores de las distintas ramas en una red única y unificada de mando y control (C2).

Alianzas militares internacionales, como la Organización del Tratado del Atlántico Norte (OTAN, 2013), han sido coherentes en importantizar la operación simultanea y coordinada en los cinco dominios actualmente reconocidos[5] y desarrolla una "noción de guerra multidominio" para dirigir a una transformación total de sus fuerzas; consiguiendo que países de la Unión Europea (UE) ya traten y hablen de la integración al multidominio en sus actualizaciones de defensa y que inicien los aprestos para ajustar sus adquisiciones, capacidades y organización a este novedoso concepto.

4 Por ejemplo, en combate, una unidad terrestre podría recibir apoyo no solo de artillería y fuerza aérea aliada, sino también de operaciones de guerra electrónica que cieguen los sensores enemigos y ataques cibernéticos contra los sistemas de mando y control enemigos.

5 Tierra, mar, aire, espacio y ciberespacio.

DOI: https://doi.org/10.59794/rscd.2025.v11i11.123

De esta manera, potencias como China inician reformas que se proponen mejorar sus capacidades en una guerra conjunta y multidominio de manera integral, y desde 2015 reorganiza sus regiones militares en comandos conjuntos, creando la Fuerza de Apoyo Estratégico que aglutina capacidades ciber, de espacio e información, adoptando una doctrina de "operaciones conjuntas integradas" con un enfoque primordial en guerra informática (Tosi, 2023). Asimismo, Rusia, independientemente de que no hace uso del término multidominio como tal en su doctrina, en la práctica demuestra una integración del enfoque al combinar la ciberguerra con ataques convencionale,[6] guerra electrónica, uso de fuerzas especiales y campañas de desinformación.[7]

Podemos ver como claramente existe un consenso en que el panorama doctrinal global indica que la superioridad militar de cualquier potencia va a depender necesaria y exclusivamente de su capacidad de llevar a cabo operaciones integrales en todos los dominios. La evolución desde "lo conjunto" a la integración multidominio ya se encuentra en marcha, sostenida por lecciones aprendidas y en curso por conflictos pasados y recientes, apoyado además por el veloz desarrollo tecnológico que indefectiblemente ha redefinido el campo de batalla que tradicionalmente conocíamos.

Lo estratégico y tecnológico: Implicaciones.

Las Fuerzas Armadas, en términos estratégicos, no solo deben planificar de forma integral, sino, que deben pensar en esos términos, teniendo en cuenta y considerando que las operaciones ejecutadas en un dominio deben y puede influir y afectar los demás dominios. Por esto podemos considerar y deducir que al adoptar un enfoque multidominio necesariamente se traduce en cambios profundos en la estrategia militar.

Como consecuencia directamente proporcional a esta, la necesidad de que los mandos conjuntos sean y estén más integrados, debiendo el mando y control (C2) estar en la capacidad de dirigir distintas unidades en todo ámbito de manera simultánea, cambiando con esto los tradicionales obstáculos entre Fuerzas. Aquellos que logren sincronizar con rapidez sus fuerzas en los múltiples dominios conseguirán tomar, mantener y explotar la iniciativa y abrumar al enemigo con la presentación de múltiples amenazas al mismo tiempo (TRADOC, 2018).

Las MDO, por sus implicaciones, desvanecen la frontera entre el conflicto, la crisis y la paz, igualmente entre lo convencional y lo no convencional, constituyéndose esto, junto a la disuasión y la escalada, en otros aspectos estratégicos característicos de este tipo de operaciones. Un ejemplo puntual puede ser el hecho de que un país emplee sus capacidades cibernéticas y/o acciones en el espacio (interferencia de satélites) en fases iniciales de un conflicto sin traspasar el umbral o la frontera de un ataque cinético tradicional.[8] Esta última forma se considera guerra híbrida o estrategias de zona gris, al combinar múltiples instrumentos, sean militares o no, con el fin de lograr objetivos políticos sin que sea desencadenada una guerra abierta (Morris et al., 2019).

6 Por ejemplo, los ataques en 2015-2017 a las redes eléctricas ucranianas.
7 En occidente se conoce como guerra híbrida al uso simultaneo de estas capacidades.
8 El término "ataque cinético" se aplica a cualquier acción destructiva que utiliza la energía cinética de un objeto en movimiento para causar daño.

Desde el punto de vista de una gran estrategia, las MDO y su integración, hacen necesario e imperativo una adecuada coordinación interagencial, entrelazando la dimensión militar con la dimensión económica, diplomática e informativa. Un ejemplo es cómo la Organización del Tratado del Atlántico Norte (OTAN, 2023), destaca el hecho de que, al aprovechar todos estos instrumentos del poder nacional en su conjunto, es vital para imponerse y lograr los objetivos en los conflictos modernos. Resumidamente, a nivel estratégico una guerra multidominio exige una orquestación y estructuración holística de las capacidades y una toma de decisiones compleja y más rápida que la de una guerra convencional y/o tradicional.

Es obvio pensar en este punto, de que el componente tecnológico, más allá de solo ser un área de competencia, es una parte fundamental y central para la ejecución de las MDO. Hay consenso en el hecho de que para poder integrar de manera efectiva múltiples dominios se hace necesario y obligatorio contar con sistemas de comunicaciones e información avanzados, así como con plataformas innovadoras y armamento con tecnología de punta.

Dentro de las implicaciones tecnológicas principales podemos mencionar cuatro vitales. La primera es la necesidad de que las redes de mando y control estén integradas y que puedan resistir los entornos hostiles.[9] La segunda es la necesidad de aplicación o uso de inteligencia artificial (IA) a los fines de que se pueda manejar con rapidez y precisión el gran volumen de datos generados en los múltiples dominios (imágenes satelitales, información e inteligencia humana, señales de radar, flujo de redes sociales, etc.).

Una tercera implicación es la adquisición y aplicación de plataformas no tripuladas y armamento de precisión, permitiendo estos sistemas[10] atacar y golpear objetivos con precisión y eficacia, reduciendo de manera considerable la exposición de las tropas propias y limitando a prácticamente al mínimo los daños colaterales y la pérdida de no combatientes y personas de la clase civil no involucradas en los conflictos. Por último, una cuarta implicación sería tanto el espacio y el ciberespacio como dominios de combate, debiendo una fuerza militar garantizar su acceso al espacio[11] y garantizar además la protección de éstos. Igualmente debe tener la capacidad y libertad de poder operar en el ciberespacio, tanto ofensiva como defensivamente, desarrollando para esto recursos humanos especializados en ciberdefensa.

A resumidas cuentas, las implicaciones tecnológicas en las MDO están determinadas tanto por la precisión como por la conectividad, esto en la ofensiva, defensiva y el mando control. Entonces podemos inferir, que la fuerza o potencia militar que haga un mejor aprovechamiento de la tecnología para atacar y defenderse contará con una ventaja considerable y se traducirá en la consecución de los objetivos planteados inicialmente.

Casos de conflictos recientes

Azerbaiyán y Armenia 2020

La segunda guerra de Nagorno-Karabaj en 2020 entre Azerbaiyán y Armenia es un conflicto que puso en evidencia las nuevas dinámicas multidominio. Con una duración de 44 días, Azerbaiyán combinó el uso intenso y constante

9 Referido a interferencias del espectro electromagnético, ciberataques, guerra electrónica, etc.
10 Misiles guiados, proyectiles inteligentes, drones aéreos, drones terrestres y vehículos aéreos no tripulados (UAVs).
11 Navegación GPS, comunicaciones satelitales, inteligencia geoespacial, etc.

de drones armados y municiones merodeadoras (kamikaze) con ciberataques propagandísticos y con ataques terrestres convencionales, logrando con esto una rápida superioridad. Los análisis sobre este enfrentamiento coincidieron en que los daños en combate fueron infligidos por plataformas no tripuladas, y que a opinión de Hertlein (2023), ha sido algo sin precedentes históricos. Por su parte Armenia, que basa sus defensas en tanques, blindados y sistemas antiaéreos tradicionales, fue abrumada prácticamente de inmediato.

Con apenas una semana de combate los drones azeríes destruyeron cientos de vehículos y sistemas antiaéreos enemigos, incluyendo modernizadas baterías de misiles s-300 (Hertlein, 2023). Al negarle a Armenia la capacidad de operar con libertad en el dominio aéreo, sus aviones casi no pudieron levantar el vuelo, y al ser empleado con destreza el dominio informativo (con publicación de videos de ataques masivos de drones para minar la moral de los armenios), Azerbaiyán estableció y creó el efecto de control multidominio local. Demostrando este caso que incluso si países pequeños integran en su doctrina tecnologías como drones se puede derrotar de manera rápida a fuerzas más tradicionales.

Rusia y Ucrania 2022-actualidad

La invasión rusa a gran escala en Ucrania en febrero de 2022 ha sido descrita como el primer conflicto en décadas entre potencias que ocurre en todos los dominios de manera intensa. Una fuerza convencional masiva rusa (tanques, artillería, aviación e infantería), se complementaron con ataques en el ciberespacio y campañas de desinformación; sin embargo, sus resultados iniciales quedaron muy por debajo de lo esperado. La falta de integración efectiva de dominios fue uno de los factores que incidieron en dicho relativo fracaso. A pesar de su potencia de fuego, Rusia no logró anular las comunicaciones ucranianas ni consiguió la supremacía aérea. Por otro lado, Ucrania aprovechó de manera creativa la guerra multidominio a su favor a pesar de tener menos medios convencionales. En el dominio cibernético Ucrania recibió gran apoyo de países y empresas aliadas para contrarrestar y resistir los ciberataques rusos. Además, utilizó con éxito la información y las redes sociales para ganar la batalla de la opinión pública mundial contrarrestando la narrativa rusa.

En el dominio espacial, Ucrania fue beneficiada de servicios como la constelación satelital Starlink para mantener las comunicaciones seguras de sus tropas en el campo de batalla, aun cuando la infraestructura tradicional fue destruida. Pudo rastrear además los movimientos enemigos a través de la obtención de inteligencia que fue proporcionada por los satélites occidentales. En el dominio aéreo, conscientes de una fuerza aérea potente, Ucrania desplegó enjambres de drones tanto de ataque como de reconocimiento (modelos militares y comerciales adaptados) para guiar la artillería con una letal precisión. En el dominio terrestre las fuerzas ucranianas demostraron una coordinación superior a nivel de unidades pequeñas, explotando su conocimiento del terreno y la inteligencia recibida para llevar a cabo contraataques efectivos.

Rusia por su lado, empleó operaciones multidominio, pero con importantes deficiencias; por ejemplo, lanzó poderosos ciberataques en paralelo con la invasión contra las redes gubernamentales ucranianas y cortes de energía eléctrica, pero la rápida respuesta ucraniana y su previa preparación limitaron su impacto. Como señala Martínez (2024), la invasión rusa ha expuesto las carencias de una estrategia híbrida mal ejecutada, mientras que la defensa

ucraniana demostró la eficacia de saber combinar recursos de múltiples fuentes en todos los ámbitos y dominios.

Israel: lecciones recientes

Israel ha sido pionero en la aplicación de principios multidominio a pequeña escala. Ya es conocido que este se encuentra rodeado de amenazas irregulares, por lo que es lógico pensar la necesidad imperante de adaptar sus operaciones a la realidad particular que enfrentan. En la guerra del Líbano de 2006 las milicias de Hezbolá sorprendieron a las fuerzas israelíes al operar en dominios inesperados: consiguieron alcanzar con un misil antibuque a una corbeta de la marina israelí (INS Hanit) durante los combates causándole daños severos. Israel admitió que subestimó la amenaza en el dominio marítimo por parte de un actor no estatal, lo que a todas luces reveló una brecha en su conciencia situacional multidominio (Harel & Issacharoff, 2008). Producto de esto Israel posteriormente reforzó su inteligencia y la integración de esta para vigilar todos los ámbitos, incluso los que anteriormente eran considerados de bajo riesgo.

En conflictos recientes como las operaciones contra Hamás en Gaza, las Fuerzas de Defensa de Israel (FDI) han combinado operaciones cinéticas de precisión (bombardeos aéreos guiados) con acciones cibernéticas y campañas informativas. Por ejemplo, durante la operación Guardián de los Muros en mayo de 2021, Israel afirmó haber frustrado intentos de hacking de Hamás contra su sistema de defensa aérea Domo de Hierro (Iron Dome), y como respuesta fue ejecutado un ataque aéreo para neutralizar los hackers adversarios, combinando así los dominios cibernéticos y aéreos. Israel utiliza una amplia y sofisticada red inteligencia humana, drones de vigilancia y análisis de señales para detectar a los lanzadores de cohetes enemigos que se encuentran ocultos entre la población civil, integrando así, el dominio informativo con el militar.

Las lecciones israelíes hacen énfasis en la relevancia de que no se debe dejar ningún dominio sin la debida atención, incluso contra enemigos asimétricos, siendo la falta de control en uno solo una brecha que conlleve a consecuencias catastróficas. Esto evidencia también la utilidad de responder en todos los dominios a las amenazas para lograr los resultados más contundentes posibles y reducir la libertad de acción del adversario.

Fuerzas Armadas de República Dominicana: retos frente a las MDO

Para el caso de la República Dominicana, país que en la actualidad no enfrenta de manera directa amenazas militares convencionales, se hace lógico preguntarse cómo se podría asumir y aplicar el concepto de MDO atendiendo a esa realidad y contexto. Primero, es de rigor mencionar que de acuerdo con la Constitución de la República Dominicana las Fuerzas Armadas dominicanas se componen por tres ramas, fuerzas y/o servicios (Ejército, Armada y Fuerza Aérea) teniendo a su cargo la defensa de la Nación, su independencia y soberanía. (Constitución de la República Dominicana, 2015). El propio texto legal además les indica participar y/o apoyar en lo referido a la seguridad interna y el apoyo a situaciones de emergencia nacional.

Sus misiones en las últimas décadas se orientan en la lucha contra el crimen organizado, el narcotráfico y la respuesta a desastres naturales y antropogénicos. Si bien es cierto que estas tareas difieren de lo que doctrinalmente se conoce como guerra convencional entre naciones,

no menos cierto es el hecho de que para llevarse a cabo requieren una coordinación e integración en múltiples dominios. Por ejemplo, la seguridad de la frontera y espacio terrestre (tierra), la vigilancia de las costas y las operaciones navales contra el contrabando (mar), patrullaje y transporte aéreo (aire), la inteligencia y la seguridad de las comunicaciones (ciberespacio) y las campañas de información pública y cooperación civil y militar (informativo).

Las Fuerzas Armadas dominicanas se han enfocado en fortalecer una estructura de mando y control conjunto, y por esto vemos como en 2020 fue inaugurado el Centro de Comando, Control, Comunicaciones, Ciberseguridad e Inteligencia (C5I) como instalación que tiene el fin de lograr la integración de los flujos de información y mejorar la toma de decisiones de las tres ramas militares y múltiples agencias gubernamentales en tiempo real.

Con esta implementación se ha conseguido gestionar de manera óptima la seguridad fronteriza y el apoyo a la Policía Nacional en lo referido a la seguridad ciudadana. Esto refleja la priorización que se le ha dado al dominio ciberespacial e informativo, y desde el Ministerio de Defensa se ha reiterado que "el ciberespacio es el quinto dominio de las operaciones militares", indicando la prioridad que tiene el proteger la información y las redes ante cualquier amenaza digital (Díaz Morfa, 2023).

En ese tenor el Ministerio de Defensa (2024), a través de la Universidad Nacional para la Defensa (UNADE) han iniciado programas de capacitación en diversos niveles sobre ciberdefensa para el personal militar y civil, incluyéndolo además como parte de los distintos programas de grado y posgrado que allí se imparten, reconociendo, evidentemente, que la Seguridad Nacional comprende también el ámbito digital. Asimismo, la cooperación internacional ha jugado un papel importante en el entrenamiento y donación de equipos que fortalezcan las FF. AA.

República Dominicana, en cuanto a los medios materiales, enfrenta el reto tecnológico de adoptar las capacidades propias de las operaciones multidominio con recursos un tanto limitados. Comparado con países mayores nuestras Fuerzas Armadas disponen con un modesto equipamiento, por ejemplo, pocos aviones de transporte y helicópteros, así como una cantidad discreta de drones, lanchas para patrullas y vigilancia costera y sistemas de radar básicos para el control aéreo. La integración de nuevas tecnologías[12] requiere de inversiones significativas y un personal altamente capacitado, no debiendo obviar el reto que conlleva además la parte doctrinal y organizacional para dicha adecuación.

No obstante, es innegable que se han dado pasos firmes y positivos encaminados a avanzar, incorporando tecnologías para el monitoreo fronterizo y modernización de las redes de radio comunicación. Pudiendo decir, en síntesis, que República Dominicana se ha ido adaptando de manera gradual a los principios de la guerra multidominio acorde a sus necesidades y capacidades.

Operaciones Multidominio: proyección.

Proyectando las MDO, evidentemente, van a seguir evolucionando a la par con los avances tecnológicos y los cambios en la manera de hacer la guerra. Para Pulido (2022), algunas

12 Drones de vigilancia, sistemas de mando y control interconectados o herramientas de ciberseguridad de última generación.

de las tendencias que se vislumbran son las siguientes:

- Sistemas autónomos y automatización, en el sentido de que la próxima generación de fuerzas va a incluir un número considerable de plataformas no tripuladas en todos los ámbitos, como enjambres de drones aéreos y terrestres, submarinos autónomos, robots de combate, etc.
- Integración total de la inteligencia artificial, no solamente en lo relativo al manejo de datos, sino en que podrá asumir funciones relevantes en la conducción de las operaciones, capaces de proponer cursos de acción en tiempo real con la simulación de escenarios para procurar adelantarse al enemigo.
- Dominio informacional y cognitivo, referente a la batalla por influir en la voluntad, percepción y toma de decisiones del contrario, con una integración mayor de operaciones psicológicas en redes sociales y campañas agresivas de desinformación.
- Militarización del espacio ultraterrestre, por la dependencia en constante crecimiento de los satélites, la navegación y la observación por medio de este tipo de tecnología, con una proliferación de satélites militares y surgimiento de armas avanzadas antisatélite.
- Operaciones hipersónicas y multidominio en tiempo real, promovido por la aparición de misiles hipersónicos[13] y plataformas de ataque de muy largo alcance, difuminando la distinción entre el frente y la retaguardia.

Las guerras del futuro tienen mucha probabilidad de que continúen por el camino de la integración multidominio, sumándose los dominios cognitivos, espacial profundo y electromagnético, añadiéndose más tecnología que va a revolucionar constantemente la forma de combatir, y que las fronteras que separan lo humano y la máquina, lo civil y lo militar, será cada vez más difusa.

Conclusiones

Hemos podido constatar cómo han evolucionado las operaciones conjuntas hacia la integración multidominio, convirtiéndose este hecho en una realidad palpable, tanto en la doctrina como en la práctica militar contemporánea. A lo largo de este escrito hemos mostrado que el concepto de guerra y operaciones multidominio ha surgido para dar respuesta a un entorno estratégico en donde ningún dominio puede operar de forma aislada y conseguir una superioridad militar frente a su enemigo, y que, por el contrario, dicha superioridad se construye a partir de la combinación de las fuerzas terrestres, navales, aéreas, espaciales, cibernéticas y cognitivas o de información de manera integral y sincronizada.

A lo largo de la historia las fuerzas armadas han transitado por medio de modelos de cooperación conjuntas relativamente simples, o sea, el apoyo aéreo al Ejército, etc., hacia modelos altamente integrados y más complejos que permiten a un comandante accionar todas las palancas que tiene a su disposición en varios dominios a la vez. Presentando un análisis doctrinal se puso en evidencia cómo conceptos anteriores y experiencias previas allanaron el camino al punto que nos encontramos hoy, representando las operaciones multidominio un salto cualitativo importante con la integración de dominios emergentes y enfoque flexibles

13 Con capacidad para maniobrar hasta cinco veces la velocidad del sonido.

ante las amenazas complejas que se han ido presentando.

La necesidad de mandos conjuntos más efectivos y con capacidad de respuesta más rápida son de las implicaciones estratégicas que se requieren, aunado a nuevos modos de disuasión y acciones en la zona gris previo a llegar a un conflicto abiertamente. En lo referido a la tecnología, queda claro que las operaciones multidominio tienen una dependencia considerablemente importante de estos sistemas avanzados de información y manejo de datos, redes de mando seguras, una rápida adopción de innovaciones (ciberdefensa, drones, IA) y de armamento de precisión.

A su nivel, la República Dominicana ha reconocido esta necesidad y ha actuado en consecuencia, dando los pasos que fortalezcan sus operaciones conjuntas y tendentes a ir reforzando su estructura para operar en múltiples dominios de manera simultánea, desarrollando la ciberdefensa, mejorando la coordinación interinstitucional y asegurando una respuesta eficaz a los retos y desafíos en su entorno. Estos cambios exigirán Fuerzas Armadas flexibles y tecnológicamente avanzadas, pero también marcos normativos éticos y doctrinales actualizados.

Finalmente, se ha de reconocer que la integración multidominio no es una "moda" y como tal pasajera, sino una evolución lógica de la forma de hacer la guerra en el siglo XXI. Las fuerzas militares que la acojan de manera integral estarán en una posición ventajosa para disuadir, y de ser necesario, prevalecer en los conflictos que han de venir.

Referencias

Borne, K. (2019). Targeting in Multi-Domain Operations. *Military Review* (ed. en español). https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2019/

Brading, T. (2021). First Multi-Domain Task Force plans to be centerpiece of army modernization. U.S. *Army News Service*. https://www.army.mil/article/242849/first_multi_domain_task_force_plans_to_be_centerpiece_of_army_modernization

Comando de Entrenamiento y Doctrina del Ejército de los Estados Unidos (TRADOC). (2018). El Ejército de los Estados Unidos en Operaciones de Múltiples Dominios 2028. *Panfleto 525-3-1 del TRADOC.*

Constitución de la República Dominicana. [Const.]. (2015). *Gaceta oficial. Núm. 10805.* Santo Domingo, República Dominicana. 10 de julio 2015. https://presidencia.gob.do/sites/default/files/statics/transparencia/baselegal/Constitucion-de-la-Republica-Dominicana-2015-actualizada.pdf

Díaz Morfa, C. (2023, 21 de octubre). Alto mando de Fuerzas Armadas se reúne en C5i para evaluar estrategia de ciberseguridad. *Listín Diario*. https://listindiario.com/la-republica/ gobierno/20231021/alto-mando-fuerzas-armadas-reune-c5i-evaluar-estrategia-ciberseguridad_778300.html

Harel, A., & Issacharoff, A. (2008). *How the navy missed its boat. Haaretz.* https://www.haaretz.com/1.4980917

Hertlein, R. M. (2023, 23 de febrero). *Commentary: Army logistics survivability against multidomain threats. Army.mil.* https://www.army.mil/article/264190/commentary_ army_logistics_survivability_against_multidomain_threats

RSC&D | Año X I / No. 11 / 2025 | ISSN:2413-869X
https://revista.unade.edu.do/index.php/rscd

King, S., & Boykin, D. B. IV. (2019, 20 de febrero). *Distinctly different doctrine: why multi-domain operations isn't airland battle 2.0. Association of the United States Army.* https://www.ausa.org/articles/distinctly-different-doctrine-why-multi-domain-operations-isnt-airland-battle-20

Manual de campo, FM 100-5: *Operaciones.* (1982). Departamento del Ejército de EE. UU. U.S. Government Printing Office.

Ministerio de Defensa. (2024). *Fuerzas Armadas capacitan civiles y militares en temas de ciberseguridad y ciberdefensa.* https://www.youtube.com/watch?v=-Dw7TzD4W8I

Morris, L., Mazarr, M., Hornung, J., Pezard, S., Binnendijk, A., & Kepe, M. (2019). *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War.* RAND Corporation. https://www.rand.org/pubs/research_reports/RR2942.html

Organización del Tratado del Atlántico Norte (OTAN). (2023, 5 de octubre). *Multi-Domain Operations in NATO – Explained.* Mando Aliado de Transformación (NATO ACT). https://www.act.nato.int/article/mdo-in-nato-explained/

Pulido, G. (2022, 28 de agosto). La guerra de Ucrania y la guerra mosaico. *Revista Ejércitos.* https://www.revistaejercitos.com/artículos/la-guerra-de-ucrania-y-la-guerra-mosaico/

Publicación *Conjunta. (2018).* Operaciones conjuntas (Manual JP 3-0). Departamento de Defensa de los Estados Unidos.

Tosi, S. J. (2023). Xi Jinping's PLA reforms and redefining "active defense." *Military Review, 103*(5), 46-57.