ESPECIALIZACIÓN EN ESTRATEGIA OPERACIONAL Y PLANEAMIENTO MILITAR CONJUNTO

TRABAJO FINAL INTEGRADOR

TEMA: La Guerra Electrónica y las acciones cibernéticas en las Operaciones Multidominio en entornos caracterizados por las Subáreas de interés estratégico.

.

AUTOR: MY Leandro Javier PALACIOS.

TUTORA: CR Abel MARRUPE PEREYRA.

AÑO: 2025

RESUMEN

El presente trabajo analiza de manera integral la relación entre la Guerra Electrónica, la Ciberdefensa y el concepto de Operaciones Multidominio dentro del marco doctrinario y legal de la República Argentina, con el propósito de evaluar el estado actual de las capacidades nacionales y los riesgos derivados de su insuficiencia. En un entorno estratégico caracterizado por la digitalización acelerada, la interdependencia de los sistemas de mando y control, la expansión del dominio cibernético y el creciente protagonismo del espectro electromagnético, la gestión de la información se ha convertido en el centro de gravedad operacional para cualquier Estado moderno. Este enfoque multidominio exige integrar simultáneamente los efectos generados en los ámbitos terrestre, marítimo, aéreo, espacial, electromagnético y cibernético, lo que implica que las capacidades de Guerra Electrónica y Ciberdefensa ya no pueden considerarse elementos complementarios, sino componentes esenciales del arte operacional contemporáneo.

El estudio se sustenta en el análisis exhaustivo del marco legal argentino, así como en doctrinas, reglamentos específicos, trabajos académicos y documentos técnicos. A partir de esta base, se examina la brecha existente entre la normativa vigente, las demandas del paradigma multidominio y la realidad tecnológica y organizacional de las Fuerzas Armadas Argentinas. Se evalúan además los riesgos operacionales y estratégicos que se derivan de la insuficiencia de capacidades, especialmente en relación con la vulnerabilidad del comando y control, la protección del espectro electromagnético, la defensa de infraestructura crítica y la capacidad de disuasión estratégica del país.

Los resultados de este análisis permiten concluir que la Argentina enfrenta un escenario complejo, donde las limitaciones tecnológicas, doctrinarias y estructurales comprometen la posibilidad de ejecutar operaciones efectivas en un entorno multidominio. En consecuencia, la investigación propone la necesidad de avanzar hacia una modernización integral de las capacidades informacionales, fortalecer la interoperabilidad conjunta, desarrollar doctrina específica, actualizar la normativa vigente y promover la autonomía tecnológica nacional como condiciones indispensables para garantizar la defensa del país y su adaptación al paradigma del siglo XXI.

PALABRAS CLAVE

Arte Operacional; Guerra Electrónica; Ciberdefensa; Operaciones Multidominio; Dominio de la Información; Infraestructuras Críticas.

INDICE

INTRODUCCIÓN

La transformación del ambiente operacional contemporáneo ha producido un quiebre decisivo en los modos tradicionales de concebir, planificar y ejecutar las operaciones militares. El desarrollo exponencial de nuevas tecnologías, la digitalización de los sistemas de comando y control, la irrupción de actores con capacidades avanzadas en el ciberespacio, y la creciente importancia del espectro electromagnético como espacio de interacción estratégica, han configurado un escenario en el cual las Fuerzas Armadas (FFAA) ya no pueden limitarse a operar en dominios tradicionales. La guerra moderna se caracteriza por su simultaneidad, su carácter no lineal, la convergencia de efectos y la creciente dependencia de sistemas interconectados. Todo ello exige la adopción de doctrinas y capacidades que permitan operar eficazmente en un ambiente disputado, dinámico y altamente competitivo.

En este contexto, las Operaciones Multidominio (MDO) se han consolidado como el paradigma doctrinario que mejor refleja la complejidad de los conflictos contemporáneos. Las mismas integran y sincronizan efectos en los dominios terrestre, marítimo, aéreo, espacial, electromagnético, cibernético e informacional, bajo una lógica que supera la conducción sectorizada y avanza hacia un modelo de empleo conjunto, coordinado y convergente. Esta concepción reconoce que la victoria ya no se obtiene mediante la supremacía en un dominio aislado, sino a través de la creación de ventajas acumulativas y sinérgicas que permitan desarticular la cohesión operacional del adversario, proteger las propias capacidades y asegurar la libertad de acción en todos los ámbitos.

La experiencia internacional demuestra que las FFAA que logran integrar eficazmente capacidades en el ciberespacio y en el espectro electromagnético incrementan de manera sustancial su capacidad de disuasión y su resiliencia estratégica. En consecuencia, el control del espectro electromagnético y la protección del ciberespacio ya no son funciones accesorias, sino elementos centrales del poder militar.

Para la República Argentina, esta realidad adquiere una relevancia particular. La posición geopolítica del país en el Atlántico Sur, su presencia en la Antártida, la extensión de su territorio, la importancia estratégica de sus recursos naturales y la creciente interconexión de sus infraestructuras críticas, configuran un escenario donde la defensa nacional depende cada vez más de capacidades tecnológicas avanzadas. Sin embargo, tal como señalan Chiavaro (2018), Herrera

(2017) y Casale (2022) en sus respectivos trabajos, el instrumento militar argentino enfrenta limitaciones significativas en materia de Guerra Electrónica (GE), Ciberdefensa (CD), comunicaciones tácticas y estratégicas, resiliencia cibernética y protección del espectro. Estas limitaciones condicionan la capacidad de ejecutar operaciones conjuntas en ambientes complejos y afectan la posibilidad de sostener la maniobra militar frente a amenazas híbridas, electrónicas o digitales.

El presente trabajo se enmarca en este contexto y busca analizar en profundidad el papel de la GE y la CD dentro del paradigma de las MDO, desde una perspectiva doctrinaria, técnica y legal, con énfasis en las necesidades, vulnerabilidades y posibilidades del instrumento militar argentino. El estudio parte de la premisa de que GE y CD no son capacidades aisladas, sino componentes estructurales del Dominio de la Información que permiten asegurar la continuidad del comando y control (C2), proteger la infraestructura crítica, garantizar la integridad de los sistemas de armas y generar efectos que condicionen la voluntad y la capacidad del adversario.

Asimismo, el trabajo se inscribe dentro del marco jurídico argentino, que establece los límites y las responsabilidades del instrumento militar en tiempos de paz y en situaciones de conflicto. Estos instrumentos normativos determinan que la defensa frente a agresiones externas es responsabilidad primaria de las FFAA, pero también establecen restricciones al empleo de capacidades en el territorio nacional.

HIPÓTESIS PRINCIPAL

¿La integración de operaciones de GE y CD en MDO, conforme al marco legal vigente, permitirá a las FFAA Argentinas incrementar su eficacia en entornos caracterizados por subáreas de interés estratégico, siempre y cuando se desarrollen y optimicen adecuadamente sus capacidades actuales y se aborden los riesgos asociados a su falta de desarrollo?

ENFOQUE METODOLÓGICO

El enfoque metodológico adoptado en este trabajo combina el análisis doctrinario, el estudio de normativa nacional, el relevamiento de trabajos académicos del ámbito militar, la evaluación de riesgos estratégicos y la integración de conceptos provenientes del arte operacional.

OBJETIVO GENERAL

Analizar y determinar las operaciones de GE y CD que pueden ejecutarse en MDO, considerando el marco legal vigente.

OBJETIVOS ESPECÍFICOS

- Examinar el marco legal y normativo que rige la participación de las FFAA para ejecutar acciones de GE y CD en MDO en entornos caracterizados por las subáreas de interés estratégico.

- Evaluar las capacidades actuales y necesarias de las FFAA Argentinas en el ámbito de la GE y la CD.

- Proponer un marco operativo para la integración de estas capacidades en MDO.

- Desarrollar un análisis de riesgos detallado sobre las implicaciones de no desarrollar adecuadamente las capacidades de GE y CD.

PERTINENCIA DEL TRABAJO

La pertinencia de este trabajo radica en la creciente amenaza que representan las capacidades electrónicas y cibernéticas de actores estatales y no estatales, así como en la vulnerabilidad tecnológica de sistemas esenciales para la defensa.

APORTE TEÓRICO PRACTICO AL CAMPO DISCIPLINAR

Este trabajo busca aportar un marco analítico sólido que permita comprender los riesgos estratégicos asociados a la falta de capacidades en GE y CD, y al mismo tiempo proponer un conjunto de lineamientos para su desarrollo futuro. En particular, se pretende demostrar que la integración doctrinaria no solo es necesario, sino urgente, para asegurar que el instrumento militar argentino pueda operar de manera eficiente y resiliente en un ambiente operacional cada vez más hostil, acelerado y tecnológicamente competitivo.

ESTRUCTURA DE TRABAJO

El trabajo se estructura en tres capítulos principales. El primero aborda el marco teórico, doctrinario y legal que fundamenta el empleo de GE y CD, integrando conceptos, así como los principales reglamentos y leyes del sistema de defensa argentino. El segundo capítulo analiza la

naturaleza de las MDO, su evolución doctrinaria, su relevancia para la Argentina y los desafíos asociados a su implementación. El tercer capítulo examina específicamente el papel de la GE y la CD como capacidades habilitantes dentro de las MDO

, evaluando su estado actual, los riesgos asociados a su insuficiente desarrollo y las posibilidades de modernización. Finalmente, el trabajo concluye con un análisis integrador que articula los hallazgos y propone recomendaciones para fortalecer la defensa nacional en el Dominio de la Información.

Capítulo I - MARCO TEÓRICO, DOCTRINARIO Y LEGAL

1.1 Introducción

La evolución del pensamiento militar a lo largo del siglo XXI ha revelado una transformación profunda en la naturaleza de los conflictos, impulsada por la tecnología, la digitalización, la conectividad global y la expansión del teatro de operaciones hacia dominios antes no contemplados. En este contexto, el arte operacional adquiere una relevancia superior, ya que se convierte en el puente entre los objetivos estratégicos y la maniobra táctica, articulando los medios disponibles para generar efectos decisivos en múltiples dominios. El arte operacional se centra en la comprensión profunda del ambiente operacional, la identificación de centros de gravedad, la articulación de líneas de operación y la creación de ventajas que permitan alterar el equilibrio estratégico. Su finalidad última es integrar capacidades de distinto nivel en una acción coherente y sinérgica, potenciando la eficacia militar.

Si bien el arte operacional mantiene elementos tradicionales como la maniobra, la sorpresa y la concentración de esfuerzos, su interpretación contemporánea incorpora conceptos derivados de la revolución de los sistemas de información, la automatización, el dominio cognitivo y la convergencia tecnológica. La guerra moderna ha dejado de ser exclusivamente una confrontación física para convertirse en un fenómeno intensamente informacional, donde el control de datos, señales, sensores y redes influye directamente sobre la capacidad del comandante para decidir y actuar. La información se integra como un recurso operacional de alto valor, transversal a todos los esfuerzos militares, lo que exige doctrinas que prioricen la gestión del espectro electromagnético y la protección de sistemas digitales.

La importancia del Dominio de la Información ha sido ampliamente reconocida por las principales doctrinas militares internacionales y es progresivamente incorporada por Argentina. En el modelo clásico, los dominios terrestre, aéreo y marítimo constituían las dimensiones fundamentales del combate; sin embargo, la aparición del dominio electromagnético y del ciberespacio ha alterado esta visión, expandiendo la guerra hacia campos no físicos que condicionan la realidad material del combate. El control del espectro y la protección de la información se vuelven elementos esenciales para sostener operaciones de cualquier tipo. La pérdida de dicho control puede traducirse en fallas en los sistemas de mando y control, interrupción de sensores críticos, degradación de enlaces satelitales y exposición de unidades a la detección enemiga.

El aporte doctrinario del Estado Mayor Conjunto (EMCO), a través del Reglamento PC 11-01, constituye un hito en la consolidación del Dominio de la Información dentro del arte operacional argentino. Este documento establece que tanto la GE como la CD deben integrarse en el ciclo completo de planeamiento operacional, desde la apreciación del ambiente hasta la ejecución y evaluación. Esta incorporación normativa eleva a la GE y a la CD a la categoría de capacidades habilitantes esenciales y no meramente complementarias. Su implementación real, sin embargo, requiere una modernización progresiva de estructuras, procedimientos, equipamiento y formación especializada.

El concepto de Dominio de la Información también se articula con la noción de guerra cognitiva, entendida como el efecto que la información tiene sobre el razonamiento, la moral, la cohesión y la toma de decisiones. Aunque este trabajo se centra prioritariamente en la dimensión técnica de la GE y la CD, la dimensión cognitiva debe reconocerse como un espacio adicional donde opera el arte operacional y donde la manipulación informacional puede producir efectos estratégicos.

La teoría del arte operacional también incorpora elementos como el diseño operacional, que consiste en identificar las relaciones causales que permiten transformar la situación inicial en una condición deseada. Para ello se utilizan herramientas como la descripción del ambiente operacional, la determinación del problema, la definición de líneas de operación, objetivos y puntos decisivos. En un entorno saturado de señales, ciberataques y desinformación, la capacidad para construir una visión operacional coherente exige que el comandante disponga de un flujo informativo confiable, protegido y oportuno. La ausencia de esta condición compromete la capacidad de realizar una evaluación estratégica objetiva, afectando potencialmente el éxito de la operación.

En la guerra moderna, la velocidad del ciclo de decisión también se ha convertido en un factor determinante. Los sistemas automatizados, la inteligencia artificial y la analítica avanzada permiten acelerar el proceso de observación, orientación, decisión y acción (ciclo OODA). Sin embargo, la eficacia de estos sistemas depende del acceso a información precisa y protegida. La interferencia o manipulación de datos puede ralentizar o bloquear el ciclo, otorgando la iniciativa al adversario. De allí que la protección de los sistemas informáticos y del espectro sea un componente irrenunciable del diseño operacional.

La integración entre el arte operacional y el Dominio de la Información también se expresa en el desarrollo de líneas de esfuerzo no cinéticas dentro de la operación. Tradicionalmente, una operación militar se caracterizaba por líneas de esfuerzo centradas en la maniobra física. En la actualidad, las operaciones integran líneas destinadas a asegurar el espectro, proteger redes, ejecutar acciones cibernéticas, obtener inteligencia multidominio y sostener la flexibilidad informacional de la fuerza. Estas acciones contribuyen de manera directa al logro de los objetivos estratégicos, aun sin emplear fuego o maniobra.

Finalmente, la evolución teórica del arte operacional revela que la información es un recurso estratégico que debe administrarse con criterios de eficiencia y seguridad. Así como en la guerra clásica se administraban reservas, líneas de suministro o posiciones, en la guerra moderna se administran datos, redes, sensores y espectro. La información se ha convertido en una dimensión logística, estratégica y operacional. Su pérdida, degradación o manipulación puede paralizar la maniobra, comprometer la seguridad y poner en riesgo la misión.

1.2 Doctrina Argentina, esquema normativo y lógica de empleo del dominio de la información.

El establecimiento doctrinario del Dominio de la Información dentro del instrumento militar argentino implica la convergencia de varios componentes: la tradición operacional del país, los documentos doctrinarios emitidos por el EMCO de las FFAA, la normativa legal que regula el accionar de las fuerzas, las políticas públicas de defensa y las prácticas que emergen de la evolución tecnológica y de la experiencia internacional. Comprender el rol de la GE y la CD requiere, por tanto, un análisis cuidadoso de la doctrina institucional vigente, su nivel de madurez, sus vacíos, las capacidades reales actualmente existentes y los desafíos que plantea su implementación operativa.

La doctrina conjunta argentina reconoce explícitamente que la información es un recurso estratégico que influye en la conducción. El Reglamento Conjunto PC 11-01 establece que la CD y la GE deben considerarse capacidades esenciales en la Acción Militar Conjunta, y enmarca su empleo dentro de principios operacionales como la oportunidad, sincronización y protección de los sistemas del C2 Este reglamento define a la Ciberdefensa como “el conjunto de acciones destinadas a prevenir, detectar, mitigar, responder y recuperarse frente a incidentes que afecten sistemas informáticos del instrumento militar”. La GE, por su parte, se organiza en funciones de

apoyo, ataque y protección, vinculadas a la manipulación del espectro electromagnético para impedir, degradar o explotar las capacidades de un adversario.

Sin embargo, la existencia doctrinal no implica automáticamente capacidad operativa. La doctrina argentina se encuentra en una fase de consolidación conceptual respecto del Dominio de la Información, pero todavía no ha alcanzado un estado pleno de integración material y funcional. Como señala Herrera (2017), "la brecha entre doctrina y capacidad puede generar falsas expectativas sobre la disponibilidad real de recursos electrónicos, sensores y equipos". La estructura de fuerzas sigue estando en proceso de modernización, con sistemas parcialmente obsoletos, capacidades heterogéneas entre las Fuerzas y limitaciones presupuestarias estructurales.

Esta brecha no invalida el desarrollo doctrinario; al contrario, lo hace imprescindible. La doctrina tiene la función de orientar la adquisición, la formación, la planificación y la integración conjunta; de allí que un marco conceptual sólido sea condición previa para la creación de capacidades modernas. La experiencia internacional demuestra que los dominios emergentes requieren cambios doctrinarios antes que tecnológicos: no es posible integrar tecnologías avanzadas sin un marco conceptual que les dé coherencia operativa. Argentina está en esa etapa, donde la consolidación doctrinaria debe guiar la modernización.

Dentro del corpus doctrinario nacional, el EMCO ha desarrollado documentos complementarios que refuerzan la importancia del Dominio de la Información. El documento "Operaciones en el Dominio de la Información" (Moresi, 2019) subraya que las fuerzas deben integrar la información en todos los niveles. Allí se afirma que "la acción militar moderna demanda la capacidad de sostener operaciones incluso bajo degradación severa del ambiente electromagnético o ante ataques cibernéticos". Esta afirmación sintetiza un principio operativo fundamental: ninguna operación militar puede prescindir del acceso seguro al espectro y a sistemas digitales confiables.

Desde la perspectiva legal, el empleo de GE y CD se encuentra condicionado por un conjunto de leyes que regulan la labor de las FFAA y su interacción con organismos civiles. La Ley de Defensa Nacional (23.554) establece que el instrumento militar sólo puede emplearse ante agresiones externas de origen estatal. Este principio tiene implicancias directas sobre la CD: una agresión cibernética puede no tener un actor estatal claramente identificado, lo que plantea dificultades para determinar el encuadre legal de la respuesta. De hecho, López (2018) advierte

que “las agresiones cibernéticas suelen ocurrir sin atribución clara, generando un vacío en la aplicación de la Ley de Defensa”. Esta ambigüedad constituye una limitación significativa que debe ser considerada en la planificación y en la formulación doctrinaria.

La Ley de Inteligencia Nacional (25.520) delimita estrictamente las funciones de los organismos de inteligencia, prohibiendo a las FFAA la realización de actividades de inteligencia interior salvo en el marco del sistema de inteligencia nacional y bajo conducción civil. Esta restricción es fundamental para evitar la militarización del ciberespacio interno. Sin embargo, al mismo tiempo dificulta la coordinación en situaciones donde la línea entre infraestructura civil y militar es difusa. Por ejemplo, los sistemas de comunicación, los enlaces satelitales, las rutas digitales y buena parte del espectro radioeléctrico pertenecen o son administrados por organismos civiles y empresas privadas. La defensa de estas infraestructuras, esenciales para la conducción militar, exige un nivel de cooperación interagencial que el marco legal debe articular explícitamente.

La Ley de Seguridad Interior (24.059) profundiza estas restricciones al establecer que las FFAA no pueden intervenir en conflictos internos o en protección directa del orden público. En el ámbito de GE y CD, esto significa que su empleo está limitado al ámbito estrictamente vinculado a agresiones externas o defensa de sistemas militares. Aunque doctrinariamente correcto, este marco presenta desafíos prácticos: la mayoría de los ciberataques que pueden comprometer sistemas militares provienen de redes civiles o son dirigidos contra infraestructuras compartidas. La frontera entre lo militar y lo civil dentro del ciberespacio es porosa, por lo que la coordinación entre organismos resulta imprescindible.

El Decreto 1112/24 constituye un avance clave, ya que reconoce explícitamente el rol del Dominio de la Información en el Sistema de Defensa Nacional. El decreto establece que la ciberseguridad es una prioridad estratégica y propone mecanismos de coordinación entre organismos del Estado para proteger infraestructuras críticas. Este reconocimiento permite sentar bases para el desarrollo de capacidades multidominio, dado que legitima la necesidad de participación militar en la protección de sistemas sensibles, siempre bajo supervisión civil. El decreto también promueve la adopción de estándares internacionales y la modernización tecnológica, elementos imprescindibles para la incorporación de capacidades GE y CD.

Otro componente doctrinario relevante es la política de protección de Infraestructuras Críticas. Sain (2019) destaca que la Argentina presenta vulnerabilidades estructurales en términos de protección de redes energéticas, de telecomunicaciones, de transporte y de servicios esenciales. Estas vulnerabilidades tienen impacto directo sobre la capacidad militar, ya que cualquier operación conjunta depende inevitablemente de rutas logísticas, centros de mando, comunicaciones y servicios energéticos que frecuentemente no pertenecen al ámbito de Defensa. En este sentido, la doctrina militar debe reconocer que la resiliencia nacional es un prerrequisito operativo.

A nivel operacional, la doctrina argentina ha incorporado la noción de ambiente operativo multidimensional. La ampliación del teatro de operaciones hacia el espectro y el ciberespacio obliga a superar visiones tradicionales centradas únicamente en dominios físicos. La doctrina debe asumir que el espectro no es un "apoyo técnico" sino un espacio de combate. Esto implica que la planificación operacional debe contemplar acciones destinadas a controlar, proteger y explotar el espectro, así como medidas para operar bajo su degradación.

Es especialmente relevante destacar que el PC 11-01 sostiene que la Ciberdefensa debe integrarse antes, durante y después de la operación. En la etapa previa, debe evaluar vulnerabilidades, diseñar medidas de protección y asegurar la integridad de sistemas críticos. Durante la operación, debe monitorear intrusiones, detectar ataques, proveer redundancias y mantener la disponibilidad de enlaces. Posteriormente, debe recuperar sistemas, análisis forenses y restablecimiento de capacidades. Esta lógica de ciclo completo se ajusta al modelo moderno de operaciones.

La GE, en tanto, debe complementarse con medidas ofensivas y defensivas. Las operaciones de ataque electrónico pueden habilitar la maniobra, mientras que las medidas de protección electrónica garantizan la supervivencia de los sistemas propios. La doctrina argentina contempla ambas funciones, pero su aplicación práctica depende de la disponibilidad de equipos modernos.

Finalmente, el marco doctrinario y legal argentino establece un equilibrio entre la protección de valores democráticos y la necesidad de modernizar el instrumento militar. La incorporación del Dominio de la Información debe respetar estos valores, garantizando control

civil, transparencia y límites claros a la intervención militar en ámbitos no estrictamente defensivos.

1.3 Relación entre doctrina, poder militar y el dominio de la información en la Argentina

La articulación entre doctrina, normativa y capacidades reales constituye un eje fundamental para comprender el grado de preparación del instrumento militar argentino frente al desafío de las MDO. En los últimos quince años, las transformaciones del ambiente estratégico global llevaron al EMCO a incluir el Dominio de la Información como una dimensión operacional esencial. Sin embargo, la capacidad real de operar en dicho dominio y de sostener la maniobra en entornos degradados permanece en desarrollo. Para comprender esta situación es necesario analizar el nivel de adaptación doctrinaria, organizacional y conceptual de las FFAA ante este nuevo paradigma.

En primer lugar, la doctrina argentina se ha visto influida por la naturaleza cambiante de la guerra y por la presión que ejercen tecnologías emergentes. El Dominio de la Información no es solo una dimensión técnica, sino un espacio donde se disputa la iniciativa. La capacidad de recopilar, procesar, distribuir y proteger información se convierte en una condición necesaria para la toma de decisiones. En este sentido, la doctrina del EMCO reconoce que la superioridad informacional constituye un centro de gravedad del instrumento militar. La pérdida de esa superioridad compromete la capacidad de conducción estratégica y operacional.

Esta perspectiva se reafirma en el PC 11-01, que define que la Ciberdefensa debe integrarse transversalmente en todo el ciclo operacional. También destaca la necesidad de evaluar vulnerabilidades de redes y sistemas antes de comenzar cualquier operación. Este componente preventivo es central, dado que la mayoría de los incidentes cibernéticos que afectan a organizaciones militares se producen por brechas de seguridad básicas o por falta de procedimientos de protección. La doctrina reconoce la existencia de esta vulnerabilidad, pero aún queda camino por recorrer para que las FFAA apliquen plenamente procedimientos estandarizados.

Por su parte, la GE ocupa un lugar destacado en el pensamiento operacional contemporáneo. La doctrina argentina considera a la GE como un medio fundamental para controlar, explotar o proteger el espectro electromagnético. Moresi (2019) señala que la capacidad de “negar, degradar o explotar señales enemigas” constituye un componente esencial para sostener el C2 en operaciones conjuntas. Sin embargo, el desafío radica en que gran parte del equipo

electrónico disponible en el país requiere modernización, lo que genera una brecha significativa respecto de las necesidades de un entorno multidominio.

La relación entre doctrina y marco legal también presenta particularidades relevantes. El modelo argentino de defensa se caracteriza por una estricta separación entre seguridad externa e interna. En muchos países, las capacidades de ciberdefensa operan de manera integrada entre organismos civiles, policiales y militares. En Argentina, en cambio, la normativa establece límites claros.

El problema se agrava debido a la dependencia del instrumento militar respecto de infraestructura civil. Los enlaces de comunicaciones, la provisión de energía, los servicios satelitales, los sistemas digitales de navegación, las redes de fibra óptica y los proveedores de servicios digitales pertenecen mayormente al ámbito no militar. Así, cualquier agresión que afecte estas infraestructuras puede degradar la capacidad de defensa sin que el instrumento militar tenga un rol definido para intervenir legalmente. López (2018) afirma que "la disociación entre responsabilidad y capacidad de acción constituye uno de los mayores desafíos en la protección del ciberespacio nacional". Para subsanar esta disociación, se requiere una política clara de coordinación interinstitucional.

El Decreto 1112/24 se aproxima a esta necesidad al introducir explícitamente la ciberseguridad como componente estratégico del Sistema de Defensa. Este avance político permite desarrollar esquemas de cooperación entre organismos, particularmente para la protección de infraestructuras críticas. Sin embargo, la efectividad real de este decreto dependerá de la capacidad del Estado para establecer estructuras permanentes de coordinación que incluyan a actores civiles, privados y militares. La naturaleza distribuida del ciberespacio exige una gobernanza compartida.

La doctrina argentina reconoce también la importancia del nivel operacional. La GE y la CD no son únicamente capacidades estratégicas o tácticas; su función principal se desarrolla en el nivel operacional, donde permiten integrar esfuerzos y sostener el diseño de la maniobra. De hecho, las MDO solo son posibles si las capacidades informacionales operan de manera coherente con las líneas de operación principales. Casale (2022) destaca que la CD debe considerarse una función operacional, ya que su rol no se limita a proteger sistemas, sino a asegurar la continuidad de la misión en situaciones de crisis.

Esta integración es especialmente relevante en el Dominio de la Información, ya que los sistemas informáticos, enlaces, antenas, sensores y dispositivos de comunicación deben operar bajo protocolos comunes para asegurar flujo de datos sin interferencias. La interoperabilidad, sin embargo, requiere inversión en sistemas, capacitación y estándares tecnológicos uniformes, aspectos aún en desarrollo.

El análisis doctrinario también revela que la cultura organizacional constituye un factor decisivo. Las FFAA están tradicionalmente organizadas bajo sistemas jerárquicos rígidos, pero el Dominio de la Información requiere flexibilidad, descentralización de decisiones y adaptación rápida.

La doctrina debe definir cómo se emplearán estos sistemas, qué prioridades se asignarán y qué nivel de redundancia será necesario para sostener operaciones en un entorno altamente disputado. La tecnología sin doctrina se vuelve ineficiente; la doctrina sin tecnología se convierte en abstracta. Por ello, el fortalecimiento doctrinario es clave para orientar la modernización futura del instrumento militar argentino.

El campo doctrinario también se relaciona con la formación profesional del personal. Las capacidades de GE y CD requieren especialistas con formación avanzada en ingeniería electrónica, telecomunicaciones, informática, criptografía y análisis forense digital. Esta formación es compleja y toma tiempo. La doctrina debe prever rutas de carrera específicas, incentivos para retener talento y mecanismos de capacitación permanente. La experiencia internacional demuestra que los recursos humanos son el componente más crítico en el Dominio de la Información.

Otro aspecto doctrinario relevante es la resiliencia. La doctrina argentina ha comenzado a incorporar el concepto de resiliencia operacional, entendido como la capacidad de sostener operaciones aun cuando el ambiente informacional está fuertemente degradado. Para ello, se requieren redes redundantes, sistemas alternativos, protocolos de “modo degradado” y procedimientos de recuperación. El pensamiento operacional moderno entiende que la resiliencia no es un atributo técnico aislado, sino un enfoque sistémico que debe orientar el diseño de la fuerza.

Finalmente, la doctrina argentina debe continuar evolucionando hacia una concepción integral del Dominio de la Información que incluya GE, CD, operaciones psicológicas, inteligencia, comunicaciones estratégicas y sistemas autónomos. Aunque este trabajo se centra en GE y CD, es importante reconocer que el dominio informacional es amplio y multidimensional.

La integración doctrinaria permitirá construir una fuerza capaz de operar de manera coordinada y efectiva en entornos de alta complejidad.

1.4 Desafíos estructurales, tecnológicos y organizacionales para la adaptación al dominio de la información en la Argentina

La consolidación del Dominio de la Información dentro del pensamiento operacional argentino exige comprender en profundidad los obstáculos que enfrenta el instrumento militar para desarrollar capacidades robustas de GE y CD. Estos desafíos no son únicamente técnicos, sino políticos, conceptuales, presupuestarios y organizacionales. La capacidad de Argentina para actuar en MDO depende del modo en que estos factores se integren de manera coherente en una estrategia nacional de defensa informacional.

El primer desafío estructural radica en la fragmentación institucional del sistema de defensa. Desde la reforma introducida por la Ley 24.948 y la actualización doctrinaria del EMCO se busca avanzar hacia un modelo conjunto, donde las decisiones operacionales se tomen desde una perspectiva integrada. Sin embargo, a nivel práctico, persisten estructuras de fuerza altamente diferenciadas entre las tres fuerzas. Esta fragmentación se refleja en la gestión de capacidades informacionales: cada fuerza conserva desarrollos propios en materia de comunicaciones, sistemas electrónicos, redes, sensores y programación. Esta diversidad dificulta la interoperabilidad real. El Dominio de la Información exige la existencia de un ecosistema común, homogéneo y estandarizado, donde los sistemas de cada fuerza puedan interactuar sin restricciones.

La interoperabilidad doctrinaria también constituye un desafío. Las operaciones modernas requieren procesos unificados de gestión de incidentes, estándares de protección, protocolos de respuesta y sistemas de autenticación. Un ataque cibernético no distingue entre jurisdicciones internas; si un vector penetra un sistema del Ejército, puede escalar hacia redes del EMCO o de la Fuerza Aérea. Por ello, la falta de doctrinas integradas incrementa el riesgo sistémico.

A nivel tecnológico, la Argentina enfrenta limitaciones significativas. El equipamiento de GE disponible en el país proviene en gran medida de desarrollos de mediados y fines del siglo XX, lo cual limita su capacidad para operar en entornos altamente densos. Los sistemas modernos de GE requieren antenas direccionales, receptores de amplio espectro, plataformas de interferencia selectiva y sistemas SIGINT de alta frecuencia. Muchos de estos equipos deben ser actualizados o

reemplazados por completo. La obsolescencia tecnológica afecta todos los niveles de la operación, desde la recolección de señales hasta la interferencia, el análisis y la protección electromagnética.

La situación es aún más compleja en el ámbito digital. Las capacidades de Ciberdefensa dependen de sistemas informáticos modernos, centros de datos, infraestructuras de procesamiento, sistemas de respaldo y redes seguras. La mayor parte del equipamiento tecnológico utilizado por el instrumento militar argentino depende de proveedores extranjeros y de estándares globales. Esto implica una dependencia estructural que limita la capacidad de improvisación ante contingencias. Además, gran parte del software utilizado no es de desarrollo propio, lo que implica riesgos tanto de seguridad como de autonomía estratégica.

Existen esfuerzos locales para revertir esta dependencia. Empresas como INVAP han desarrollado sistemas de radarización que permiten ampliar las capacidades de vigilancia. Sin embargo, la integración de estos desarrollos al Dominio de la Información requiere inversiones complementarias en procesamiento de datos, ciberseguridad, comunicaciones y análisis en tiempo real. Un radar que detecta amenazas aéreas no resulta útil si la red que transmite la información es vulnerable a ataques. De esta manera, la modernización de la tecnología militar debe ser entendida como un proceso integral.

Otro desafío fundamental es el factor humano. La formación de este tipo de especialistas requiere tiempo, recursos y un diseño curricular avanzado. Las academias militares han comenzado a actualizar sus planes de estudio, pero la velocidad de los cambios tecnológicos supera la capacidad de adaptación institucional. Además, el mercado civil compite por los mismos perfiles profesionales, ofreciendo condiciones económicas que las FFAA difícilmente pueden igualar.

La retención de talento constituye uno de los puntos críticos más delicados del sistema de defensa argentino. Los oficiales y suboficiales que adquieren conocimiento avanzado en ciberseguridad o ingeniería informática son frecuentemente tentados por empresas privadas de tecnología, bancos, aseguradoras o firmas internacionales. La rotación del personal especializado genera un círculo vicioso: el Estado invierte en formación, pero pierde a los recursos más capacitados, lo que debilita la continuidad operativa. Para revertir esta situación, se requieren políticas de incentivos, carreras específicas y reconocimiento profesional acorde a la sofisticación técnica de las tareas.

En otro sentido la Ley de Seguridad Interior limita la participación militar en asuntos de ciberseguridad que involucren redes civiles. Dado que la mayor parte de las infraestructuras informáticas pertenecen al ámbito privado, las FFAA pueden intervenir solo en casos excepcionales con autorización del Poder Ejecutivo. Esta limitación produce "zonas grises" donde un incidente cibernético que afecta infraestructura dual o crítica no puede ser abordado eficientemente. La dependencia de redes civiles sin un mecanismo claro de intervención legal constituye una vulnerabilidad estructural.

La Argentina carece de una política nacional de ciberseguridad plenamente integrada con la defensa. Existen estrategias dispersas entre distintos ministerios, agencias y organismos. Esta dispersión dificulta la coordinación, lo cual es especialmente crítico en el Dominio de la Información, donde los ataques se propagan en cuestión de segundos. La falta de un organismo centralizado que coordine acciones de defensa cibernética entre lo civil y lo militar reduce la capacidad del Estado para responder ante amenazas sofisticadas.

La ciberseguridad no debe ser vista como una actividad reactiva. Las amenazas modernas se caracterizan por operaciones persistentes y encubiertas. Grupos estatales y no estatales realizan infiltraciones profundas que pueden permanecer latentes durante meses o años antes de activarse. Por ello, la defensa debe ser proactiva, con monitoreo constante, inteligencia de amenazas, auditorías periódicas, actualización de sistemas y redundancias operativas. La doctrina argentina reconoce esta realidad, pero su implementación completa aún no ha sido alcanzada.

La articulación entre GE y CD es esencial para lograr efectos sinérgicos. La GE permite degradar sistemas enemigos, mientras que la CD protege los propios y explota debilidades adversarias. En un entorno multidominio, ambas capacidades deben operar de manera coordinada. Una operación de interferencia electrónica solo resulta efectiva si se integra con acciones cibernéticas que exploten vulnerabilidades emergentes. De igual manera, una intrusión cibernética puede potenciarse mediante el control del espectro electromagnético. Esta integración requiere una visión sistémica que aún está en proceso de consolidarse en el instrumento militar argentino.

El futuro de la defensa argentina dependerá en gran medida de la capacidad del Estado para modernizar sus herramientas y adaptar su doctrina a este nuevo paradigma. La inversión en tecnología debe ir acompañada de reformas institucionales, programas de formación y actualizaciones normativas. No basta con adquirir equipamiento; es necesario desarrollar una

cultura organizacional que entienda el valor estratégico de la información. La guerra moderna se libra en todos los dominios, pero la victoria se decide en el terreno informacional.

La complejidad del Dominio de la Información exige que el Estado construya una arquitectura de defensa integral. Esto incluye fortalecer alianzas internacionales, participar en ejercicios combinados, mejorar la cooperación entre organismos civiles y militares, fomentar el desarrollo científico y tecnológico nacional y promover la industria de defensa. La autonomía estratégica en materia informacional requiere capacidad de desarrollo propio. La dependencia de proveedores externos puede convertirse en una vulnerabilidad crítica durante una crisis.

Finalmente, la modernización del Dominio de la Información en Argentina no debe ser vista como un lujo tecnológico, sino como una necesidad estratégica. La competencia global, el avance de tecnologías disruptivas y la creciente sofisticación de las amenazas convierten a la CD y la GE en elementos esenciales de la seguridad nacional. La protección del Estado, sus instituciones y su soberanía depende de la capacidad de operar con eficacia en este dominio. La transformación es inevitable; la cuestión es si se realizará con la velocidad suficiente para responder a los desafíos del siglo XXI.

1.5 Conclusión Parcial del Capítulo I

El análisis realizado en este capítulo permite comprender que la GE y la CD constituyen pilares indispensables del arte operacional contemporáneo, especialmente dentro del paradigma de las MDO. El marco doctrinario nacional, aunque presenta avances significativos, aún se encuentra en un proceso de adaptación frente a las exigencias del entorno estratégico actual, donde la información, el espectro electromagnético y el ciberespacio se configuran como elementos decisivos para la superioridad operacional. Asimismo, el marco legal argentino ofrece una estructura normativa sólida para la defensa nacional, pero requiere actualizaciones que integren explícitamente la dimensión informacional en todas sus expresiones. La conjunción de doctrina, legislación y necesidades operacionales demuestra que existe una brecha entre la teoría y las capacidades reales del instrumento militar, lo que fundamenta la necesidad de profundizar el desarrollo conceptual y normativo en materia de GE y CD. Esta conclusión parcial permite afirmar que sin una comprensión integral del dominio de la información y sin su incorporación plena en la doctrina y en el sistema legal argentino, la transición hacia MDO continuará limitada y fragmentada.

CAPÍTULO II - Guerra Electrónica y Ciberdefensa en Operaciones Multidominio

2.1 Base conceptual, evolución histórica y relación con el arte operacional

La comprensión de la GE y la CD como capacidades esenciales dentro del diseño de la maniobra moderna exige un análisis profundo y articulado acerca de su evolución conceptual, histórica y operacional. En el contexto argentino, el desafío de integrar estas capacidades al nivel operacional dentro de un esquema de MDO representa tanto una necesidad estratégica como una oportunidad doctrinaria. Este capítulo examina, desde una perspectiva amplia, cómo la GE y la CD constituyen herramientas indispensables para alcanzar la superioridad informacional y asegurar la libertad de acción del comandante en un ambiente operacional caracterizado por la complejidad, la simultaneidad y la convergencia de efectos militares.

La GE y la CD no surgieron de manera aislada, sino que son producto del progresivo desplazamiento del centro de gravedad de los conflictos hacia el dominio informacional. A lo largo del siglo XX, el espectro electromagnético comenzó a ocupar un papel cada vez más relevante en la conducción de operaciones militares. Durante la Segunda Guerra Mundial, el uso de radares, comunicaciones interceptadas y contramedidas electrónicas demostró que el control del espectro constituía una ventaja decisiva. La evolución posterior, marcada por la Guerra Fría, consolidó la idea de que la capacidad de interceptar señales, interferir comunicaciones y proteger sistemas propios era un componente central del poder militar. Con el surgimiento de las redes digitales en las décadas de 1980 y 1990, la dimensión cibernética expandió exponencialmente el alcance del dominio informacional.

En este sentido, la distinción clásica entre GE, centrada en el espectro electromagnético, y Ciberdefensa, enfocada en redes, sistemas y datos, se vuelve insuficiente para describir la dinámica actual del conflicto. Ambas capacidades convergen en un mismo propósito: obtener, preservar y explotar la información como recurso estratégico. Esta convergencia está reflejada en doctrinas contemporáneas y especialmente en debates actuales de seguridad internacional. Pulido (2021) sostiene que las guerras multidominio “transforman la forma en que se integran los efectos militares, al requerir la sincronización simultánea de acciones en lo terrestre, aéreo, naval, espacial, cibernético e informacional”. Para lograr dicha integración, la GE y la CD no pueden ser concebidas como funciones aisladas, sino como ejes transversales del diseño operacional.

El análisis histórico de la GE demuestra que esta disciplina ha acompañado la evolución del arte operacional desde sus orígenes. En la Primera Guerra Mundial, la intercepción de comunicaciones permitió anticipar movimientos enemigos. En la Segunda Guerra Mundial, la interferencia de radares condicionó operaciones aéreas y marítimas. En conflictos recientes como Kosovo, Irak y Ucrania, la capacidad de negar el espectro electromagnético ha sido un factor decisivo para desorganizar las líneas de mando y control adversarias. La Ciberdefensa, por su parte, adquirió notoriedad estratégica a partir del ataque a Estonia en 2007, que evidenció que un país puede ser paralizado sin que un solo proyectil sea disparado.

En el contexto argentino, la GE y la CD se vinculan estrechamente con la necesidad de proteger la soberanía, garantizar la libertad de acción del instrumento militar y asegurar la continuidad de las comunicaciones estratégicas. La geografía del país, incrementa la importancia del dominio informacional. La interrupción de enlaces satelitales, la interferencia de redes de comunicación o un ciberataque contra infraestructuras energéticas podrían comprometer severamente la capacidad del Estado para responder a amenazas externas.

Las MDO exigen una comprensión integrada de las capacidades informacionales. No basta con interferir señales enemigas o proteger redes propias; es necesario sincronizar efectos. La clave de las MDO radica en su capacidad de generar dislocamientos sistémicos sobre un adversario mediante la convergencia de efectos simultáneos provenientes de diversos dominios. La GE puede degradar la conciencia situacional enemiga, mientras la CD explota una vulnerabilidad digital, la inteligencia electrónica recolecta información crítica y las plataformas terrestres o aéreas maniobran en consecuencia. Global Strategy (2022) destaca que el enfrentamiento multidominio “rompe la linealidad clásica de las operaciones militares al integrar efectos simultáneos que afectan decisores, sistemas y estructuras del adversario”. Esta perspectiva coincide con la visión doctrinaria contemporánea del EMCO.

El carácter multidominio redefine la importancia del tiempo dentro del proceso operacional. La velocidad de procesamiento informacional, la capacidad de análisis, la reacción ante incidentes digitales y la rápida adaptación del espectro electromagnético son factores que influyen directamente en la iniciativa. En un conflicto moderno, unos pocos segundos pueden determinar la pérdida de un sistema crítico. Por ello, la GE y la CD son las herramientas que permiten garantizar esa fluidez frente a un adversario que buscará permanentemente degradarla.

Las MDO también incorporan una dimensión cognitiva. La información no solo se utiliza para apoyar la maniobra, sino también para influir sobre percepciones, decisiones y comportamientos. Esto implica que las capacidades de GE y CD deben integrarse con la inteligencia, la comunicación estratégica y, eventualmente, con operaciones psicológicas. Aunque este trabajo se centra específicamente en GE y CD, es imposible comprender su impacto operacional sin tener en cuenta el rol de la información en la toma de decisiones adversarias. La doctrina argentina ha comenzado a reconocer esta interdependencia, pero aún existe un camino amplio por recorrer en materia de integración orgánica.

Finalmente, es necesario destacar la importancia que la GE y la CD tienen para la resiliencia operacional. La capacidad de mantener operaciones bajo degradación informacional se convierte en un objetivo estratégico. Un comandante no puede depender exclusivamente de un sistema digital centralizado; debe contar con redundancias, canales alternativos y procedimientos establecidos para operar en un entorno donde la información puede ser interrumpida, manipulada o falsificada. La resiliencia no es solamente una propiedad técnica, sino una mentalidad operacional que debe permear toda la estructura militar. En este sentido, Ortiz (2024) señala que la capacidad de adaptación informacional constituye "un factor decisivo para sostener la iniciativa táctica y operacional en entornos altamente disputados".

2.2 Integración operacional de la Guerra Electrónica y la Ciberdefensa: funciones, roles, efectos y empleo.

La integración de la GE y la CD dentro de operaciones militares constituye uno de los desafíos más significativos del diseño operacional moderno. Su valor no radica únicamente en la capacidad técnica de interferir, proteger o explotar información, sino en su rol para permitir, sostener y potenciar la maniobra militar en todos los niveles de conducción. En un entorno multidominio, donde los sistemas están interconectados y la velocidad de transmisión de datos se convierte en un factor decisivo, el empleo coordinado de GE y CD se transforma en un requisito indispensable para obtener y mantener la superioridad informacional.

En primer lugar, es necesario comprender que la lógica de las MDO obliga a abandonar concepciones lineales del conflicto. La fricción ya no se expresa únicamente en el terreno físico, sino que se produce en la esfera digital y electromagnética. Las acciones en el espectro y en el ciberespacio tienen efectos inmediatos sobre la maniobra terrestre, aérea, naval o espacial. De esta

manera, la integración operacional de la GE y la CD no responde a un esquema secuencial, sino a una convergencia simultánea de esfuerzos orientados a generar inestabilidad en los sistemas adversarios. Según Pulido (2021), las MDO "desestabilizan al enemigo a través de la sincronización de efectos provenientes de múltiples dominios que afectan su estructura, su proceso decisorio y su capacidad de respuesta". Esta perspectiva coincide con los planteamientos de Global Strategy (2022), que describe el enfrentamiento multidominio como una ruptura deliberada del equilibrio adversario mediante presiones simultáneas en diversos niveles y dimensiones.

En el nivel estratégico, la GE y la CD constituyen instrumentos esenciales para sostener la disuasión y proteger la infraestructura crítica del Estado. La conducción estratégica debe asegurar que las redes institucionales, los sistemas de comunicaciones interministeriales, los enlaces satelitales y la arquitectura digital nacional permanezcan operativos ante agresiones externas. Esto incluye la continuidad del sistema nacional de comando, la protección de los sistemas financieros, energéticos y de transporte, así como la defensa de la infraestructura digital que permite el funcionamiento del Estado. En este nivel, la CD adquiere una dimensión política, dado que un ataque cibernético puede afectar directamente la gobernabilidad y estabilidad del país. Como señala López (2018), la capacidad estatal de responder a ataques informacionales "se convierte en un componente esencial de la soberanía y de la credibilidad del sistema político y militar". Esto implica que las FFAA, dentro de los límites legales existentes, deben proteger sus redes y sistemas, coordinarse con organismos civiles y contribuir a la resiliencia nacional.

La GE, en el ámbito estratégico, se orienta principalmente a preservar la integridad de las comunicaciones estratégicas y a asegurar la disponibilidad de sensores estratégicos. Argentina depende de sistemas satelitales, radares de vigilancia, estaciones terrenas, redes integradas de comunicaciones y plataformas aéreas para mantener su conciencia situacional nacional. La interferencia o neutralización de estos sistemas podría afectar severamente la capacidad del Estado para ejercer control sobre su propio territorio. Por ello, la doctrina nacional exige la existencia de planes permanentes de protección electromagnética, protocolos de redundancia y procedimientos de recuperación ante degradación.

En el nivel operacional, las capacidades de GE y CD adquieren un rol central dentro del diseño de la maniobra. La conducción operacional debe integrar estas capacidades en el planeamiento desde la fase inicial, definiendo objetivos, efectos, sincronización y prioridades. El

propósito principal en este nivel es garantizar la libertad de acción del comandante, permitir la maniobra conjunta y degradar la capacidad adversaria para ejecutar sus propias operaciones. La GE, en este nivel, se orienta a controlar el espectro electromagnético, asegurando que las comunicaciones propias funcionen mientras se niega acceso al adversario. Esto puede incluir acciones de interferencia contra radares, comunicaciones, enlaces satelitales, sistemas de navegación y sensores tácticos.

La CD, en el nivel operacional, tiene como función proteger los sistemas C2, los centros de operaciones, las redes logísticas, las plataformas automatizadas y los sistemas de información utilizados para la planificación. Durante operaciones conjuntas, la degradación de un centro de operaciones puede generar caos en el flujo de órdenes, provocar retrasos y comprometer la cohesión de las fuerzas. Por ello, la CD no solo debe reaccionar ante ataques, sino anticiparse a ellos, identificar vulnerabilidades, realizar auditorías continuas, reforzar puntos críticos y establecer capas de defensa múltiples para reducir el riesgo de intrusión o explotación adversaria. Casale (2022) sostiene que la CD debe ser entendida como "una función operacional destinada a garantizar la continuidad del ciclo de planeamiento y ejecución, incluso bajo condiciones de degradación informacional".

El valor de la integración GE y CD radica en su capacidad para generar efectos cruzados. Una operación de interferencia puede abrir una ventana para un ataque cibernético. Un ataque digital puede desconfigurar sistemas que luego serán localizados mediante inteligencia electrónica. Esta interacción exige una coordinación centralizada en el nivel operacional y una ejecución descentralizada en el nivel táctico. La doctrina argentina ya reconoce esta complementariedad, pero su implementación plena requerirá cambios estructurales en procedimientos, equipos, formación y cultura organizacional.

La integración también implica sincronizar tiempos y efectos. En un entorno multidominio, una operación de GE debe coordinarse con acciones terrestres, aéreas, navales o cibernéticas. Por ejemplo, la interferencia de un radar enemigo debe coincidir con la maniobra aérea que pretende ocultarse. La neutralización cibernética de un sistema de artillería debe sincronizarse con la maniobra terrestre que explotará la brecha generada. Global Strategy (2022) enfatiza que la clave del enfrentamiento multidominio es la "sincronización temporal de efectos convergentes que desbordan la capacidad de adaptación del adversario". Para que esta sincronización sea efectiva,

la estructura de mando debe contar con sistemas de comunicaciones confiables, personal altamente capacitado y una doctrina clara que establezca responsabilidades, procedimientos y niveles de autoridad.

Es importante destacar que la integración operacional de la GE y la CD es un proceso gradual que requiere madurez institucional, inversiones sostenidas y una visión estratégica a largo plazo. La doctrina argentina avanza en este camino, no obstante, la tendencia global indica que los Estados que no desarrollen plenamente estas capacidades tendrán dificultades para operar en entornos de alta complejidad tecnológica. En este sentido, la Argentina debe continuar fortaleciendo su doctrina, estructuras, sistemas y personal para garantizar su capacidad de actuar eficazmente en el siglo XXI.

2.3 Capacidades requeridas, brechas existentes, evaluación de riesgo para la Argentina

La construcción de capacidades robustas de GE y CD en el marco de MDO exige una evaluación detallada de las necesidades reales del instrumento militar argentino, así como de las brechas estructurales, doctrinarias, tecnológicas y organizacionales que actualmente limitan su eficacia.

El punto de partida para este análisis radica en reconocer que las MDO exigen un nivel de integración tecnológica y doctrinaria muy superior al que requieren las operaciones conjuntas tradicionales. Las MDO son esencialmente operaciones de convergencia: reúnen efectos simultáneos provenientes de múltiples dominios con el fin de desestabilizar la estructura del adversario, paralizar sus procesos decisorios y degradar su capacidad de respuesta (Pulido, 2021). Para ello, se requiere un conjunto de capacidades informacionales que permitan detectar, anticipar, influir y neutralizar acciones enemigas con velocidad y precisión. Estas capacidades no solo deben existir, sino también integrarse adecuadamente a los sistemas de mando y control (C2), a los procesos de planeamiento y a la ejecución conjunta de operaciones.

En el caso de la GE, las capacidades requeridas incluyen la detección y análisis de emisiones electromagnéticas, la interferencia de comunicaciones adversarias, la protección de sistemas propios mediante medidas electrónicas defensivas, y la explotación de señales para obtener inteligencia. Estos elementos constituyen la base de la superioridad electromagnética. Sin embargo, la disponibilidad de equipamiento moderno, sensores avanzados, sistemas de alerta electrónica y plataformas que permitan actuar en profundidad es limitada en la Argentina. Moresi

(2019) señala que “el país enfrenta un rezago en materia de sistemas de GE que afecta directamente la capacidad de operar en un espectro electromagnético altamente disputado”. La dependencia de sistemas heredados de décadas anteriores y la falta de modernización tecnológica reducen significativamente la efectividad del instrumento militar argentino frente a amenazas que explotan vulnerabilidades del espectro.

En cuanto a la Ciberdefensa, las capacidades requeridas son incluso más amplias y complejas. La CD moderna requiere la existencia de sistemas de protección perimetral, monitoreo constante de redes, inteligencia de ciberamenazas, análisis forense digital, equipos de respuesta a incidentes y arquitecturas redundantes que aseguren la continuidad operativa. Además, requiere personal especializado capaz de operar sistemas avanzados, detectar patrones anómalos, identificar intrusiones persistentes, mitigar vulnerabilidades y coordinar acciones de defensa activa. Sin embargo, como indica Herrera (2017), la Argentina enfrenta dificultades significativas para consolidar equipos profesionales altamente capacitados, debido tanto a la competencia del mercado laboral civil como a la falta de estructuras militares diseñadas específicamente para retener talento especializado.

Este contexto deriva en una serie de brechas estructurales que afectan la preparación del instrumento militar argentino en el Dominio de la Información. Una de las brechas más significativas es la ausencia de interoperabilidad plena entre las FFAA. A pesar de los avances doctrinarios promovidos por el EMCO, las Fuerzas conservan sistemas, procedimientos y doctrinas internas que no siempre son compatibles entre sí. Esta falta de interoperabilidad, señalada también por Ortiz (2024), se refleja en la imposibilidad de integrar datos en tiempo real, compartir información sin restricciones o actuar bajo una arquitectura unificada de mando y control. Las MDO requieren una integración profunda entre dominios que solo puede lograrse si todos los sistemas, procedimientos y doctrinas operan de manera coherente y sincronizada.

Otra brecha crítica se relaciona con la dependencia de infraestructura civil para sostener sistemas militares. Las FFAA dependen de redes civiles de fibra óptica, proveedores privados de servicios digitales, satélites comerciales, redes estatales mixtas y sistemas energéticos que no están diseñados específicamente para sostener operaciones militares bajo ataque. López (2018) afirma que esta dependencia constituye “una vulnerabilidad estructural que compromete la capacidad militar de operar bajo condiciones de agresión informacional”. En un escenario de conflicto, esta

dependencia podría traducirse en interrupciones severas, pérdida de comunicaciones esenciales o fallas en sistemas críticos.

La falta de redundancias operativas también constituye un riesgo significativo. La resiliencia informacional requiere la existencia de enlaces alternativos, sistemas duplicados, operaciones en modo degradado y protocolos claros para mantener la cohesión del comando. Sin estos elementos, un ataque cibernético exitoso o una interferencia electrónica bien ejecutada, puede paralizar el funcionamiento de un comando operacional. En términos doctrinarios, la resiliencia es una condición esencial para sostener la maniobra dentro de entornos degradados (EMCO, 2019), pero en la práctica no existen suficientes redundancias para garantizarla.

Otro factor de vulnerabilidad está vinculado a la ausencia de una política nacional unificada de ciberseguridad plenamente integrada con la defensa. Existe un conjunto de iniciativas aisladas y organismos dispersos, pero no una estructura coherente capaz de coordinar acciones civiles y militares ante una amenaza cibernética significativa. Esta falta de integración limita la capacidad de respuesta, ya que las amenazas informacionales suelen dirigirse simultáneamente a sectores civiles, privados y militares. Las MDO exigen una coordinación estrecha entre el instrumento militar y el resto del aparato estatal, pero la legislación argentina limita la participación militar en redes civiles, lo que obstaculiza la construcción de una defensa integral.

La carencia de ejercicios militares específicos es otra brecha relevante. Si bien existen ejercicios conjuntos orientados a operaciones tradicionales, las prácticas que integran GE y CD en escenarios multidominio son escasas. Los países que lideran este campo realizan ejercicios regulares que simulan perturbaciones del espectro electromagnético, ataques cibernéticos y degradación severa de comunicaciones. La ausencia de simulaciones avanzadas limita la capacidad de las FFAA Argentinas para desarrollar una verdadera cultura operacional informacional.

Las consecuencias derivadas de estas brechas pueden visualizarse claramente al analizar escenarios operacionales probables. Un escenario típico podría involucrar acciones hostiles en zonas de interés estratégico, como el Atlántico Sur o la frontera norte del país. En estos escenarios, un adversario podría emplear drones, interferencia GPS, ataques cibernéticos contra infraestructura energética o manipulación de comunicaciones. La falta de redundancias, equipos modernos de GE y personal especializado podría comprometer la capacidad argentina para detectar, responder y contrarrestar estas acciones.

Otro escenario plausible es un ataque contra infraestructuras críticas civiles, como plantas energéticas o redes de transporte, con el objetivo de crear caos interno y limitar la capacidad del Estado para movilizar su instrumento militar. La falta de integración plena entre organismos civiles y militares dificultaría una respuesta coordinada. En este caso, las FFAA podrían proteger sus sistemas internos, pero el Estado en su conjunto podría entrar en crisis, afectando indirectamente la capacidad militar operacional.

Un tercer escenario implicaría la manipulación informacional o ataques contra sistemas satelitales. La dependencia de satélites extranjeros para comunicaciones estratégicas convierte estos sistemas en blancos atractivos. La GE y la CD deben ser capaces de proteger enlaces críticos y de operar sin ellos en caso de pérdida temporal. Sin embargo, la falta de sistemas alternativos independientes reduce la capacidad argentina de sostener la operación en entornos de alta degradación informacional.

En todos estos escenarios, la ausencia de capacidades informacionales robustas incrementa el riesgo operativo y estratégico. La doctrina argentina reconoce esta situación al destacar que la superioridad informacional es una condición necesaria para el éxito militar (Moresi, 2019). Sin embargo, la velocidad de evolución de las amenazas supera la velocidad de adaptación nacional, generando una brecha que debe ser atendida con urgencia.

En síntesis, la Argentina enfrenta un conjunto de desafíos estructurales y tecnológicos que limitan su capacidad para operar con eficacia en entornos multidominio. Las brechas identificadas en este bloque constituyen riesgos significativos para la defensa nacional. La construcción de capacidades de GE y CD requiere inversión sostenida, reformas doctrinarias, actualización normativa, fortalecimiento de recursos humanos y la consolidación de una arquitectura nacional de ciberseguridad integrada. El análisis de estas brechas y escenarios permite comprender la gravedad del riesgo que enfrenta el Estado en un mundo donde el dominio informacional se convierte progresivamente en el espacio decisivo para el ejercicio del poder militar.

2.4 Análisis comparado e integración de conceptos

El análisis integral de la GE y la CD en el marco de las MDO adquiere mayor claridad cuando se contrasta la realidad argentina con las experiencias internacionales. Aunque cada país diseña su arquitectura informacional de acuerdo con su historia, presupuesto, amenazas y estructura institucional, existen patrones comunes que permiten identificar buenas prácticas,

modelos de referencia y tendencias tecnológicas y doctrinarias ampliamente aceptadas. En este sentido, el análisis comparado constituye una herramienta valiosa para evaluar el grado de preparación nacional y para orientar la evolución futura del instrumento militar argentino en el Dominio de la Información.

En primer lugar, los Estados que han alcanzado mayor desarrollo en materia de GE y CD implementan modelos integrados de ciberseguridad nacional, donde los sectores militar, civil y privado trabajan bajo marcos de cooperación estables. Países como Estados Unidos, Israel, Reino Unido, Francia y Corea del Sur han creado estructuras nacionales permanentes dedicadas al monitoreo del ciberespacio, la protección de infraestructuras críticas, la respuesta ante incidentes y la coordinación de capacidades conjuntas. El caso estadounidense es particularmente ilustrativo, ya que el U.S. Cyber Command se organiza como un comando unificado con autoridad plena sobre operaciones cibernéticas ofensivas y defensivas, integrada estrechamente con capacidades electrónicas y espaciales. Esta integración permite sincronizar efectos en múltiples dominios con precisión y velocidad, lo que constituye un requisito fundamental para la ejecución de MDO. En estos países, la CD y la GE no son capacidades auxiliares, sino pilares centrales de la maniobra multidominio.

En contraste, la Argentina mantiene una separación rígida entre defensa y seguridad interior, derivada de su marco normativo. Si bien este modelo responde a un contexto histórico particular, limita la capacidad del Estado para integrar respuestas amplias ante amenazas híbridas. La fragmentación de competencias dificulta la consolidación de un comando unificado que coordine GE, CD, inteligencia, comunicaciones estratégicas y protección de infraestructuras críticas. Como señala Ortiz (2024), “la falta de coordinación interinstitucional “reduce significativamente la capacidad del Estado para responder a amenazas que se desarrollan en dominios superpuestos y que requieren sincronización inmediata”. Por ello, un desafío clave para la Argentina radica en avanzar hacia esquemas de cooperación reforzada que respeten su marco legal pero que permitan mayor interoperabilidad entre instituciones.

Otra característica común en los países avanzados es la inversión sostenida en desarrollo tecnológico. La modernización de GE depende de sensores sofisticados, sistemas de interferencia inteligentes, antenas avanzadas, plataformas aéreas y satelitales, inteligencia artificial aplicada al espectro electromagnético y sistemas de análisis automatizado. Del mismo modo, la CD moderna

requiere software propio, hardware soberano, centros de datos seguros, redes militares independientes, sistemas de criptografía nacional y herramientas de análisis forense avanzadas. La Argentina ha realizado avances significativos en áreas específicas, sin embargo, estas capacidades no se encuentran plenamente integradas dentro de una arquitectura operativa que permita su uso dentro de MDO. Gran parte de los sistemas de comunicaciones y software militar dependen de proveedores extranjeros, lo que compromete la autonomía estratégica. Moresi (2019) afirma que la disponibilidad de equipamiento propio "constituye un factor esencial para garantizar la seguridad de las operaciones militares". La dependencia externa puede convertirse en una vulnerabilidad crítica en un conflicto de alta intensidad.

Además de la adquisición de tecnología, los países avanzados han comprendido que la clave del Dominio de la Información reside en el capital humano. La formación de especialistas altamente capacitados, la creación de carreras profesionales específicas, la actualización constante en nuevas tecnologías y la retención del talento son elementos esenciales de cualquier estructura de defensa moderna. Estados como Israel y Estonia construyeron modelos exitosos basados en el desarrollo de recursos humanos desde edades tempranas, integrando a estudiantes, académicos, reservistas y profesionales expertos dentro de ecosistemas de innovación que alimentan directamente a las capacidades militares y de seguridad nacional. En América Latina, países como Brasil han avanzado notablemente en la consolidación de una arquitectura nacional de ciberseguridad que articula organismos civiles y militares bajo estructuras coordinadas.

En comparación, la Argentina enfrenta dificultades significativas para retener especialistas en GE y CD. La competencia del mercado laboral civil, las restricciones presupuestarias y la ausencia de carreras específicas dentro de la estructura militar contribuyen a la pérdida constante de talento. Herrera (2017) destaca que "la rotación del personal especializado constituye una amenaza directa para la continuidad de los programas de modernización informacional". Por ello, la consolidación de un cuerpo profesional estable y altamente capacitado es uno de los desafíos más urgentes para el país.

Otro aspecto relevante del análisis comparado es la existencia de ejercicios combinados que integran GE y CD en escenarios operacionales complejos. Los países líderes realizan simulaciones regulares para medir la resiliencia de sus sistemas, evaluar la coordinación interinstitucional y poner a prueba la integración de efectos multidominio. Estos ejercicios

incluyen interferencia GPS, simulación de ataques cibernéticos, degradación masiva del espectro, compromisos simultáneos en diversos dominios y manipulación informacional. La Argentina participa esporádicamente en ejercicios combinados, pero carece de una estructura sistemática de entrenamiento informacional que permita desarrollar una verdadera cultura de MDO. Casale (2022) subraya que "la ausencia de entrenamiento específico limita la capacidad de la fuerza militar para actuar con eficacia en entornos altamente disputados". La implementación de simulaciones avanzadas constituye, por lo tanto, un componente esencial de cualquier política de modernización.

El análisis comparado permite identificar un conjunto de recomendaciones estratégicas para la Argentina. En primer lugar, es necesario fortalecer la doctrina conjunta en materia de GE y CD, integrando estas capacidades como funciones transversales del diseño operacional. La doctrina debe establecer procedimientos claros para la integración de GE y CD en todas las fases de las operaciones, definir responsabilidades y niveles de autoridad, y promover la interoperabilidad entre las tres fuerzas. En segundo lugar, se requiere una modernización tecnológica sostenida que permita reducir la dependencia de proveedores externos. Esto implica inversiones en desarrollo nacional, alianzas estratégicas con organismos internacionales y la creación de consorcios tecnológicos que integren al sector privado, la academia y las FFAA. En tercer lugar, la Argentina debe avanzar hacia un modelo de gobernanza nacional del ciberespacio que permita coordinar acciones civiles y militares sin violar los límites legales existentes. La cooperación interinstitucional, el intercambio de información y la coordinación de respuestas son elementos indispensables para enfrentar amenazas híbridas. En cuarto lugar, el país debe desarrollar un plan nacional de formación y retención de talento informacional, creando incentivos, carreras técnicas militares específicas y mecanismos para integrar a expertos civiles en estructuras de defensa.

2.5 Conclusión parcial del capítulo II

La GE y la CD constituyen los pilares fundamentales del Dominio de la Información y se integran como capacidades esenciales dentro de las MDO. El análisis desarrollado en este capítulo demuestra que la Argentina enfrenta un conjunto de desafíos estructurales, tecnológicas, doctrinarios y humanos que limitan su preparación para enfrentar amenazas modernas. Sin embargo, también evidencia que existen oportunidades significativas para modernizar el instrumento militar mediante una combinación de reformas doctrinarias, inversión en tecnología,

fortalecimiento de capital humano y cooperación interinstitucional. La superioridad informacional no es un estado permanente, sino una condición que debe construirse y sostenerse continuamente mediante la innovación, el adiestramiento y la integración multidominio. En este sentido, el fortalecimiento de las capacidades de GE y CD constituye una prioridad estratégica para la defensa nacional y para la inserción de la Argentina en el escenario internacional contemporáneo.

CAPÍTULO III - RIESGOS ESTRATÉGICOS PARA LA ARGENTINA ANTE LA INSUFICIENCIA DE CAPACIDADES DE GE Y CD EN OPERACIONES MULTIDOMINIO

3.1 Introducción

La ausencia o insuficiencia de capacidades de GE y CD dentro del instrumento militar argentino representa uno de los mayores riesgos estratégicos que enfrenta el país en el siglo XXI. A diferencia de las amenazas tradicionales, que se expresaban a través de la violencia física o el empleo directo de fuerzas militares convencionales, las amenazas informacionales se caracterizan por su invisibilidad, su velocidad y su enorme capacidad disruptiva. En el marco de las MDO, la capacidad de agredir en el espectro electromagnético o en el ciberespacio permite a un adversario alterar procesos esenciales del Estado, paralizar infraestructuras críticas, desorganizar redes militares y generar efectos desproporcionados sin necesidad de establecer contacto físico con el territorio nacional. Esta transformación del conflicto, ampliamente analizada en el campo de los estudios estratégicos contemporáneos, exige que la Argentina evalúe en profundidad el riesgo sistémico asociado a su falta de preparación en el Dominio de la Información.

El riesgo no deriva únicamente de la posibilidad de un ataque directo, sino de la combinación de factores externos e internos que incrementan la vulnerabilidad estructural del Estado. En primer lugar, el escenario estratégico regional y global muestra un crecimiento sostenido de actores estatales y no estatales que emplean herramientas informacionales como parte de su estrategia de poder. Los conflictos recientes, como la guerra entre Rusia y Ucrania, han demostrado que las MDO comienzan mucho antes de que se produzcan enfrentamientos físicos. La manipulación de redes, la interferencia de comunicaciones, la explotación de vulnerabilidades digitales y el uso de ataques cibernéticos coordinados constituyen el prólogo de cualquier confrontación militar moderna. Global Strategy (2022) destaca que el enfrentamiento avanzado en MDO se caracteriza por “la convergencia temprana de efectos que buscan degradar la percepción,

la capacidad de decisión y la cohesión del adversario incluso antes del inicio formal del conflicto". Este modelo muestra la centralidad del Dominio de la Información como espacio decisivo.

En el caso argentino, esta realidad se vuelve particularmente crítica debido a la dependencia creciente de sistemas tecnológicos para garantizar la continuidad del Estado. La administración pública nacional, los servicios de defensa, las infraestructuras energéticas, los bancos, los aeropuertos, la navegación aérea, los ferrocarriles, los sistemas satelitales y las redes provinciales de gobierno dependen en gran medida de sistemas digitales que pueden ser alterados, interrumpidos o manipulados a distancia. Esta dependencia incrementa el impacto potencial de cualquier agresión informacional y convierte al ciberespacio en un espacio de vulnerabilidad nacional. Como señala López (2018), "la vulnerabilidad informacional del Estado argentino constituye una amenaza directa para su capacidad de ejercer control y proteger el funcionamiento de sus instituciones fundamentales".

Desde la perspectiva militar, el riesgo se amplifica al considerar que las FFAA mantienen una dependencia significativa de redes civiles y sistemas tecnológicos que no han sido diseñados para soportar situaciones de guerra informacional. Las operaciones conjuntas, los centros de comando y control, los enlaces tácticos, la logística, la inteligencia y la coordinación estratégica requieren comunicaciones estables, sistemas encriptados y arquitecturas de protección avanzadas. La ausencia de redundancias o la existencia de redes vulnerables puede provocar que un ataque cibernético dirigido, o incluso una interferencia electromagnética relativamente limitada, provoque un colapso temporal de la capacidad operativa del instrumento militar.

En este contexto, la falta de capacidades robustas de GE y CD se convierte en un riesgo estratégico de primer orden. La guerra moderna no concede margen para improvisación técnica. Un país que carece de la capacidad para defender su infraestructura digital, proteger su espectro electromagnético o reducir la vulnerabilidad de sus sistemas enfrenta un riesgo existencial, dado que un adversario puede, sin necesidad de invadir el territorio, alterar el funcionamiento del Estado, bloquear redes esenciales, paralizar procesos militares y comprometer la seguridad nacional en su conjunto. Esta situación no es teórica: numerosos países han experimentado ataques cibernéticos que han afectado infraestructuras esenciales sin que se produjeran enfrentamientos militares directos.

La insuficiencia de capacidades de GE tiene consecuencias igualmente graves. La pérdida temporal del control del espectro electromagnético puede afectar la conducción operacional de manera inmediata. La interferencia de comunicaciones tácticas, la degradación de sistemas de navegación GPS, la interferencia contra radares terrestres o aéreos, y la manipulación de sensores pueden limitar la maniobra y generar incertidumbre en el campo de batalla. Las MDO exigen operar en entornos altamente disputados donde el espectro está bajo presión constante. Sin capacidades adecuadas, las fuerzas argentinas podrían quedar ciegas, sordas o desconectadas en medio de una operación crítica.

El riesgo estratégico para la Argentina también se expresa en la pérdida de credibilidad internacional. Un país que no puede garantizar la seguridad de sus sistemas informacionales puede ser percibido como un actor débil, lo que afecta su capacidad para construir alianzas, participar en operaciones combinadas o asumir compromisos internacionales de seguridad. La falta de capacidades en el Dominio de la Información reduce la capacidad del país para actuar de manera autónoma y para garantizar su defensa ante amenazas tecnológicamente avanzadas.

Finalmente, el riesgo no debe analizarse solamente desde una perspectiva militar, sino desde una perspectiva sistémica. En un mundo interdependiente, los ataques informacionales no se limitan a un dominio. Una agresión cibernética contra un banco puede generar efectos económicos que afecten al Estado. Una interferencia contra infraestructura energética puede paralizar la movilización militar. La falta de capacidades de GE y CD afecta no solo al instrumento militar, sino a la defensa nacional en su conjunto.

3.2 Riesgos operacionales para la Argentina en Operaciones Multidominio

La modernización del campo de batalla ha transformado radicalmente la naturaleza del riesgo militar. En las MDO, los riesgos derivados de la insuficiencia de capacidades de GE y CD se expresan de forma simultánea en distintos niveles de conducción, afectando directamente la maniobra táctica, la conducción operacional y la estrategia nacional. Esta multiplicidad de efectos convierte a la vulnerabilidad informacional de la Argentina en un riesgo sistémico.

El riesgo operacional, constituye uno de los niveles más críticos para la Argentina. La conducción operacional integra las fuerzas tácticas dentro de una maniobra conjunta más amplia. Este nivel depende de centros de comando, redes de comunicaciones estratégicas, sistemas de inteligencia, enlaces satelitales, vigilancia aérea y terrestre, y plataformas de mando que

centralizan información proveniente de múltiples dominios. La insuficiencia de capacidades de GE y CD puede provocar que un adversario degrade o interrumpa completamente la capacidad de conducción operacional, afectando el flujo de información entre escalones, alterando la distribución de fuerzas y comprometiendo la coordinación entre las tres FFAA.

La interferencia electrónica a nivel operacional puede afectar directamente radares de largo alcance, sensores estratégicos, estaciones terrenas satelitales y sistemas de GE propios. La pérdida temporal de estas capacidades reduce drásticamente la conciencia situacional y la capacidad del comandante operacional para anticipar movimientos adversarios. Como destaca Moresi (2019), "la superioridad informacional es un requisito indispensable para sostener la libertad de acción operacional" (p. 22). En ausencia de esta superioridad, la maniobra conjunta se vuelve vulnerable, lenta y predecible.

En el ámbito cibernético, el riesgo operacional es aún más profundo. Un ataque dirigido a centros de operaciones, servidores críticos, redes logísticas o sistemas de planificación puede paralizar la conducción operacional. La Argentina, como muchos estados modernos, depende de sistemas interconectados que sostienen la logística, la administración del personal, la planificación de operaciones y el procesamiento de inteligencia. La intrusión en uno de estos sistemas puede generar un efecto dominó. Casale (2022) señala que "la pérdida de sistemas de mando y control tiene la capacidad de desorganizar completamente la maniobra conjunta en cuestión de minutos". La insuficiencia de capacidades de CD hace que este tipo de riesgos no solo sean posibles, sino altamente probables en un conflicto moderno.

La insuficiencia de capacidades informacionales en la Argentina genera riesgos decisivos en todos los niveles de conducción militar. Desde la pérdida de cohesión táctica hasta la erosión de la estabilidad institucional, los efectos de esta vulnerabilidad son profundos, amplios y sistémicos. Estos riesgos no solo afectan la capacidad del instrumento militar, sino la integridad y continuidad del Estado. En el siguiente bloque se desarrollarán escenarios prospectivos aplicados, con el propósito de visualizar cómo estos riesgos pueden materializarse en la práctica.

La integración de los análisis tácticos, operacionales y estratégicos desarrollados permiten comprender la profundidad y el carácter sistémico de los riesgos que enfrenta la Argentina en el marco de las MDO. El Dominio de la Información se ha convertido en el eje articulador de la acción militar contemporánea, y su degradación provoca efectos en cascada que pueden

comprometer la libertad de acción, la continuidad del mando, la cohesión social e incluso la estabilidad institucional del Estado. En este bloque se presenta una síntesis comprehensiva de estos riesgos, integrando el análisis doctrinario, legal y técnico con una perspectiva prospectiva orientada a la toma de decisiones estratégicas.

La crisis estructural que enfrenta la Argentina en materia de GE Y CD tiene raíces profundas en la discontinuidad de políticas tecnológicas de largo plazo, la obsolescencia de los sistemas existentes, la dependencia externa para el sostenimiento de capacidades críticas y la falta de un enfoque multidominio plenamente integrado. Este conjunto de limitaciones configura una vulnerabilidad esencial: la incapacidad del Estado para sostener operaciones militares en un entorno caracterizado por niveles crecientes de competencia en el espectro electromagnético y cibernético. En conflictos recientes analizados por Pulido (2021), por ejemplo, se observa que la supremacía informacional ha sido decisiva en las fases iniciales de la confrontación y ha condicionado la capacidad del adversario para movilizar fuerzas o sostener una defensa efectiva.

La insuficiencia de capacidades tácticas en GE y CD implica que las unidades desplegadas carecen de medios robustos para proteger sus comunicaciones, detectar interferencias o sostener la integridad de sus sistemas de navegación, sensores o enlaces digitales. Esta vulnerabilidad táctica, que podría parecer limitada en su alcance, es en realidad el primer eslabón de una cadena de efectos que se amplifica a medida que la degradación avanza hacia niveles operacionales. La pérdida de comunicaciones tácticas, la manipulación de datos en drones de reconocimiento o la interferencia de sistemas GPS no solo afecta la maniobra de pequeñas unidades, sino que altera la imagen operacional que recibe el comandante y genera un cuadro situacional incompleto o corrupto, lo cual compromete decisiones críticas. Esta dinámica ha sido señalada por Moresi (2019), quien afirma que “la integridad de la información es un componente esencial de la maniobra operacional”.

En el nivel operacional, el riesgo se multiplica, porque la conducción conjunta depende de sistemas interconectados cuya falla simultánea puede paralizar la maniobra militar. El instrumento militar argentino utiliza infraestructuras digitales mixtas, donde sistemas militares conviven con redes civiles y servicios provistos por actores privados. La ausencia de un ecosistema de seguridad robusto, combinado con la antigüedad y heterogeneidad de los sistemas existentes, crea una vulnerabilidad acumulativa. En este contexto, un ataque cibernético o una campaña de

interferencia electrónica dirigida contra centros de comando conjunto, servidores logísticos o sistemas de análisis de inteligencia podría generar una interrupción funcional de la capacidad de comando. Casale (2022) advierte que "la pérdida temporal del flujo informacional en el nivel operacional tiene efectos que pueden resultar irreversibles durante el desarrollo de una operación conjunta". Esto significa que la Argentina podría perder el control de la maniobra militar aún antes de que se produzca un enfrentamiento directo.

La dimensión estratégica del riesgo es aún más decisiva, porque en el paradigma multidominio el adversario no necesita destruir al instrumento militar en el terreno para obtener una ventaja decisiva; basta con paralizar la estructura informacional del Estado. Los ataques cibernéticos y electrónicos dirigidos contra infraestructuras críticas, instituciones financieras, redes energéticas, comunicaciones gubernamentales o medios de transporte pueden producir un colapso funcional que afecte la capacidad del país para movilizar recursos militares, coordinar acciones interministeriales o sostener una operación prolongada. Esta lógica ha sido ampliamente estudiada por López (2020), quien sostiene que "la pérdida de la soberanía informacional tiene un impacto directo en la capacidad del Estado para ejercer el poder nacional en su conjunto". En este sentido, la insuficiencia de capacidades de GE y CD compromete no solo la defensa, sino la gobernabilidad.

La vulnerabilidad estratégica se amplifica por la creciente dependencia argentina de proveedores extranjeros para la gestión de satélites, sistemas digitales, software crítico y tecnologías de encriptación. Esta dependencia tecnológica genera un riesgo doble: por un lado, implica la posibilidad de que actores externos tomen decisiones que afecten la disponibilidad de servicios esenciales para la defensa; por otro, expone al país a interferencias o intrusiones derivadas de fallas o vulnerabilidades no detectadas en sistemas de origen extranjero. Chiavaro (2018) subraya que la autonomía tecnológica es un pilar indispensable para garantizar la libertad de acción estratégica, especialmente en el Dominio de la Información.

Es evidente que un adversario podría explotar las vulnerabilidades informacionales argentinas para desarrollar campañas multidominio que integren desinformación, interferencia electrónica, sabotaje cibernético, operaciones psicológicas y maniobras convencionales. Los ataques podrían desarrollarse de manera simultánea en múltiples dominios, con un impacto acumulativo capaz de colapsar funciones estratégicas en cuestión de horas. Global Strategy (2022)

explica que “la velocidad de decisión en MDO define la capacidad de un Estado para mantener el control del conflicto”. Sin capacidades informacionales avanzadas, la Argentina quedaría relegada a un rol reactivo, siempre un paso detrás del adversario.

La evaluación integrada del riesgo demuestra que la insuficiencia de capacidades de GE y CD constituye un riesgo de carácter sistémico porque atraviesa transversalmente todos los niveles de conducción, afecta funciones esenciales del Estado y puede producir efectos en cascada que no pueden ser controlados por medios puramente militares. El riesgo multidominio argentino no es solo tecnológico; es organizacional, doctrinario e institucional. El marco legal vigente, establece principios para la acción del Estado, pero no logra abarcar plenamente los desafíos multidominio contemporáneos. La ausencia de una doctrina actualizada que integre el Dominio de la Información en la planificación operacional limita aún más la capacidad del país para anticipar, mitigar o responder a riesgos complejos.

En síntesis, la Argentina enfrenta un riesgo multidominio integral que exige la modernización urgente de sus capacidades de GE y CD. La protección del Dominio de la Información es una condición indispensable para garantizar la continuidad operacional, la seguridad estratégica y la estabilidad institucional del país. El instrumento militar argentino debe avanzar hacia un modelo integrado, resiliente y autónomo que le permita enfrentar amenazas cada vez más sofisticadas y operar eficazmente en un entorno caracterizado por la competencia permanente entre actores estatales y no estatales.

3.3 Conclusiones del CAPÍTULO III

En conclusión, el Capítulo III demuestra que la insuficiencia de capacidades de GE y CD constituye una amenaza estructural que compromete la defensa nacional, la estabilidad institucional y la autonomía estratégica del país. La Argentina enfrenta un riesgo que no puede ser mitigado con soluciones parciales o fragmentadas; requiere una estrategia integral de modernización informacional que articule los niveles táctico, operacional y estratégico dentro de un enfoque multidominio plenamente consolidado. Solo así podrá garantizarse la seguridad del Estado y la continuidad operativa del instrumento militar en los escenarios complejos del siglo XXI.

CONCLUSIONES FINALES

El análisis integral desarrollado a lo largo de este trabajo permite afirmar con claridad que la GE Y CD constituyen capacidades críticas, imprescindibles e impostergables para garantizar la defensa de la República Argentina en el contexto de las MDO. El estudio demostró que el Dominio de la Información se ha consolidado como el centro de gravedad de las confrontaciones contemporáneas, reconfigurando de manera decisiva el modo en que los Estados planifican, ejecutan y sostienen operaciones militares. La transformación del entorno estratégico internacional exige un instrumento militar capaz de operar en escenarios crecientemente complejos y altamente tecnificados.

El trabajo evidenció que la Argentina enfrenta una situación de vulnerabilidad estructural en el Dominio de la Información, derivada de múltiples factores: la heterogeneidad de sus sistemas de vigilancia y comunicaciones, la obsolescencia de parte de su infraestructura tecnológica, la falta de capacidades específicas en GE y CD, la dependencia de proveedores extranjeros, la insuficiente consolidación doctrinaria en MDO, y la ausencia de una integración plena entre los distintos organismos responsables de la defensa y la seguridad informacional. Esta vulnerabilidad no es meramente técnica; es institucional, doctrinaria y estratégica. Su persistencia compromete la libertad de acción del instrumento militar y limita la capacidad del Estado para garantizar la protección de sus intereses vitales.

El estudio concluye también que la normativa vigente constituye un marco imprescindible para la acción estatal, pero resulta insuficiente para abarcar la complejidad contemporánea. Es necesaria una actualización doctrinaria y legal que reconozca explícitamente la centralidad del Dominio de la Información, la naturaleza dual de las amenazas cibernéticas, la integración civil-militar en infraestructura crítica y la necesidad de coordinación interagencial permanente.

Finalmente, el análisis permitió identificar que la evolución del instrumento militar argentino hacia un modelo multidominio robusto requiere de una estrategia nacional de desarrollo tecnológico sostenido, inversión en capacidades de GE y CD, fortalecimiento de la industria nacional, creación de doctrinas actualizadas, formación especializada del personal y establecimiento de estructuras permanentes para la protección, monitoreo y control del Dominio de la Información. El país necesita avanzar hacia la construcción de una autonomía estratégica

informacional que permita garantizar la defensa de la soberanía, sostener la continuidad del Estado y asegurar la estabilidad institucional frente a amenazas complejas.

En síntesis, este trabajo demuestra que la modernización de capacidades de GE Y CD no es una opción futura, sino una necesidad presente. La defensa nacional, en el siglo XXI, depende de manera decisiva de la capacidad del Estado para proteger, controlar y explotar el Dominio de la Información. La Argentina se encuentra frente a un punto de inflexión estratégico: avanzar hacia un modelo de defensa moderno, integrado y resiliente, o enfrentar un escenario de vulnerabilidad creciente que comprometerá su capacidad de respuesta, su estabilidad y su soberanía. El desafío es ineludible, y su resolución condicionará el lugar del país en el sistema internacional durante las próximas décadas.

BIBLIOGRAFIA

Casale, M. (2022). *La Ciberdefensa como factor crítico en el desarrollo de Operaciones Militares en el Nivel Operacional*. Escuela Superior de Guerra.

Casale, M. (2022). *Convergencia de las Operaciones de Guerra Electrónica y Ciberdefensa para su empleo dentro de un Teatro.* Escuela Superior de Guerra Conjunta.

Chiavaro, J. (2018). *LA INFLUENCIA DE LA GUERRA ELECTRÓNICA EN EL DISEÑO OPERACIONAL*. Escuela Superior de Guerra Conjunta.

Herrera, A. (2017). *DISEÑO Y PLANIFICACIÓN DE LAS ACTIVIDADES DE GUERRA ELECTRÓNICA EN EL AMBIENTE OPERACIONAL*. Escuela Superior de Guerra Conjunta.

Moresi, F. (2019). *Operaciones en el Dominio de la Información*. Escuela Superior de Guerra.

Ortiz, N. (2024). *La importancia de la Ciberdefensa y la Guerra Electrónica a nivel Táctico en el marco de las Operaciones Multidominio*. Escuela Superior de Guerra.

Pulido, G. (2021). *Guerra multidominio y mosaico*. Revista de Estudios Estratégicos.

Vergara, J. (s.f.). *CAVIII - OMC*. Escuela Superior de Guerra.

Estado Mayor Conjunto. (2019). *PC 11-01 Reglamento de Ciberdefensa y Guerra Electrónica para la AMC*.

Ministerio de Defensa. (2024). *Decreto 1112/24 – Sistema de Defensa Nacional*.

Global Strategy. (2022). *El enfrentamiento avanzado: las operaciones multidominio*. de https://global-strategy.org

Grupo Oesia. (2023). *Guerra electrónica: el campo de batalla silencioso del futuro*. de https://grupooesia.com

Congreso de la Nación Argentina. (1988). *Ley 23.554 de Defensa Nacional*. Boletín Oficial de la República Argentina.

Congreso de la Nación Argentina. (1991). *Ley 24.059 de Seguridad Interior*. Boletín Oficial de la República Argentina.

Congreso de la Nación Argentina. (2001). *Ley 25.520 de Inteligencia Nacional*. Boletín Oficial de la República Argentina.