TRABAJO FINAL INTEGRADOR

TEMA:

LA ESTRUCTURA TIPO DE UN COMANDO OPERACIONAL.

TÍTULO:

LA ORGANIZACIÓN DE LA JEFATURA DE INTELIGENCIA DEL COMANDO OPERACIONAL DE LAS FUERZAS ARMADAS EN LAS OPERACIONES MULTIDOMINIO.

ARENAS, Enzo

Año 2021

RESUMEN

La creación del comando operacional de las fuerzas armadas forma parte del proceso de conjuntes en el que se vieron inmersa las fuerzas armadas argentinas a partir de la guerra por las Malvinas y particularmente desde la reglamentación de la ley de defensa nacional. Dicho comando permite la conducción de las operaciones militares conjuntas operativas y administrativas en tiempo de paz, pero además en el caso de un conflicto, también ejercerá la conducción hasta tanto se conforme el comando del teatro de operaciones. Este comando se encuentra estructurado con un estado mayor coordinador, en el cual la jefatura de inteligencia en su organización ha quedado desactualizada no solo para enfrentar conflictos de carácter convencional, sino además aquellos que en la actualidad se destacan por ser asimétricos, híbridos y desarrollarse en los ámbitos físicos y no físicos, por lo que no permite producir la inteligencia necesaria para apoyar la toma de decisiones en las operaciones multidominio.

Este trabajo busca analizar las diferentes doctrinas sobre las operaciones en los dominios que han tomado preponderancia en los últimos tiempos, como son las ciberoperaciones y las operaciones de información. Las doctrinas para el análisis serán las de las fuerzas armadas de España comparadas con la de las fuerzas armadas de Argentina.

Asimismo se analizaran las disciplinas de inteligencia que deberán ser explotadas en la jefatura de inteligencia, desde la disciplina de inteligencia humana pasando por la inteligencia de fuentes abiertas hasta la ciberinteligencia.

El propósito de esta investigación es determinar la conformación del órgano de dirección de inteligencia de un comando estratégico operacional que permita apoyar a la toma de decisiones en ámbitos que no son solo físicos sino además en los dominios cibernéticos y cognitivos.

La estructura de esta jefatura de inteligencia no solo permitirá asesorar y asistir a la toma de decisiones en las operaciones militares durante la paz, sino servirá de base para replicar la organización del órgano de dirección inteligencia del comando de un teatro de operaciones que va a ser el instrumento militar que con mayor frecuencia desarrollara las operaciones en el multidominio.

Palabras claves.

Multidomino – Inteligencia – Comando – Ciberinteligencia - Información

ÍNDICE

INTRODUCCIÓN

Frente a las distintas misiones y responsabilidades, el comando operacional constituye un estado mayor coordinador que comprende la totalidad de los campos de la conducción y aquellos necesarios para establecer el estado mayor especial y La conformación del comando operacional de las fuerzas armadas argentinas a partir del año 2007, tiene la misión de conducir las operaciones militares en tiempo de paz, proponer y desarrollar el planeamiento operacional y conducir las operaciones militares en situación de crisis y hasta tanto se cree el comando estratégico operacional (Estado Mayor Conjunto de las Fuerzas Armadas, 2020, apartado dependencias). Además dirige las actividades que lleva a cabo el comando conjunto antártico, propone la incorporación de medios ajenos a las fuerzas armadas que permitan la ejecución de las misiones operacionales impuestas, ejecuta el adiestramiento alistamiento y despliegue de los elementos conjuntos y combinados en el marco de las misiones militares de paz bajo mandato de la organización de las naciones unidas y por ultimo asesora y asiste al jefe del estado mayor conjunto de las fuerzas armadas en materia de estrategia operacional y planeamiento de estrategia militar.

Asimismo uno de los conceptos que abarca la evolución de los conflictos actuales, fundamentados en el avance de la tecnología, es el de las operaciones multidominio, concepto acuñado por el ejército de los Estados Unidos, que permite distinguir los cinco dominios o ámbitos en los cuales se desarrollan las operaciones militares, a los que al dominio terrestre, aéreo y marítimo, se incorporan el de uso satelital asociado al ciberespacio y el dominio de la información a través de la opinión pública y el enjambre de conectividad.

Dentro del estado mayor general la jefatura de inteligencia tendrá la responsabilidad, entre otras, de conducir el planeamiento de inteligencia, orientar y coordinar el esfuerzo de obtención de información y de las medidas de seguridad de contrainteligencia de nivel estratégico operacional (Estado Mayor Conjunto de las Fuerzas Armadas, 2007, pp.13-14). Además la jefatura de inteligencia deberá mantener actualizada la situación de inteligencia en aquellos lugares donde son desplegadas fuerzas militares de paz u observadores militares, requerir la información e inteligencia necesaria al estado mayor conjunto de las fuerzas armadas para desarrollar el planeamiento de apoyo a las zonas de emergencias y a la conducción de las operaciones de las fuerzas armadas en el marco del sistema federal de emergencia en la Argentina y en países de la región, man-

tener actualizada la información que permita ejecutar las actividades de apoyo a la comunidad como es el apoyo de telecomunicaciones a infraestructuras críticas de información y los enlaces necesarios que permitan asegurar el flujo de información pertinente y oportuno para los casos de emergencia.

La descripción de las anteriores responsabilidades y actividades requieren el desarrollo de operaciones no solo en los dominios tradicionales sino en aquellos dominios, como son el espectro satelital, el ciberespacio y el dominio cognitivo. Ante esto, el comando operacional constituye un estado mayor en el cual la jefatura de inteligencia no está conformada con los departamentos y divisiones que permitan abarcar las disciplinas de inteligencias suficientes, entendiendo como estas a la inteligencia humana, de imágenes, de señales, técnica, geoespacial, de fuentes abiertas, contrainteligencia y ciberinteligencia; que permitan producir la inteligencia necesaria en las operaciones de características multidominio.

En la actualidad dicha jefatura se encuentra en un proceso de conformación basado en la doctrina de un comando de un teatro de operaciones, pero esta doctrina no contempla las diferentes operaciones que en estos tiempos llevan adelante las fuerzas armadas argentinas y que se desenvuelven en el multidominio. Una muestra de esta falencia, es que no dispone de un elemento que produzca la información y emita los requerimientos en la disciplina de ciberinteligencia.

Contexto histórico

La jefatura de inteligencia como elemento de asesoramiento y asistencia que forma para de un estado mayor coordinador emplea, desde la creación del comando operacional en el año 2007, una estructura que se replica en las unidades y grandes unidades de las diferentes fuerzas armadas en la Argentina. Tanto en los estados mayores del Ejército, la Armada y la Fuerza Aérea, el ciclo de la producción de inteligencia para asesorar y asistir a sus respectivos comandos, es el mismo, y es aquel que las fuerzas armadas occidentales, vienen utilizando desde el año 1948 apoyados en la teoría del profesor Sherman Kent y de los Tenientes Coroneles Robert Glass y Phillip Davidson sobre la inteligencia estratégica, la misma estableció como método para la producción de inteligencia, al llamado ciclo de inteligencia y que es utilizado por el sistema de inteligencia en la República Argentina, desde el nivel estratégico nacional, estratégico militar, estratégico operacional hasta el nivel táctico, siendo el nivel estratégico operacional de inteligencia, el que sirve de análisis para el estudio de esta investigación.

Dicho ciclo de inteligencia que expresan en su obra, “Inteligencia para los Comandantes” (Glass y Davidson, 1948, p. 16) permite ordenar el proceso para la producción de inteligencia en una recurrencia de pasos, estos se componen por la dirección, la obtención, el procesamiento y la posterior difusión a los usuarios que se sirvan de la inteligencia producida bajo el concepto de necesidad de saber. En tanto Sherman Kent, siguiendo este ciclo, profundizó y formalizó el proceso del ciclo de inteligencia y su metodología analítica, sentando las bases que conciben a la inteligencia como una actividad intelectual y esencialmente analítica, según lo expresa en su libro de inteligencia estratégica (Kent, 1951, pp. 170-171), insistiendo en que la inteligencia, no es solo secretos, sino más bien, que el análisis de la misma puede apoyarse en información que no sea secreta y se encuentra en fuentes abiertas. En una segunda línea de pensamiento que propugnaron, Sherman Kent y los Tenientes Coroneles Glass y Davidson, es la distancia, en términos de honestidad intelectual, que debe existir entre quien toma la decisión y quien proporciona el asesoramiento, esto es, entre el comandante operacional y el órgano de dirección de inteligencia estratégico operacional. Esta separación, se distingue para preservar la integridad y la objetividad de la inteligencia como producto, evitando de esta manera que el análisis y el analista sean próximos a lo que el comandante desea oír, según lo expresa la contribución académica de la cátedra de inteligencia estratégica (Campos, 2019, p.31). Esta línea de pensamiento permite determinar cuál es el enfoque teórico al cual estarán circunscriptos los procesos y sistemas de producción de inteligencia que deben ser empleados para apoyar a la toma de decisiones de un comando operacional.

Tradicionalmente las operaciones militares han implicado la compartimentación entre los diferentes espacios en los cuales actúan cada fuerza, para los que necesitan cierto grado de especialización, a estos espacio se ha dado por llamarlos ámbitos, entornos y por ultimo dominio (Academia de las Ciencias y las Artes Militares, 2020, p.2). Asimismo cada fuerza debe tener la capacidad de maniobra y lograr objetivos y efectos de nivel estratégico. Estos dominios como son el terrestre, aéreo y marítimo que hasta la primera guerra mundial no generaba demasiada controversia, pero que a partir de la segunda guerra mundial aparecieron nuevos dominios difícil de reconocer por no ser estos de naturaleza física. El primer dominio en aparecer fue el espectro electromagnético, posteriormente el empleo del ciberespacio y por ultimo lo que se llama dominio cognitivo o de la información. Estos dominios fueron considerados en un principio como secundario a los dominios tradicionales o llamados físicos, debido a que no era po-

sible realizar operaciones, ejecutar maniobras o conseguir objetivos estratégicos en los mismos.

En los últimos años esto ha sufrido un cambio importante en el desarrollo de las operaciones militares en donde los dominios denominados no físicos o intangibles han tomado una preponderancia, de manera que poseen tanta trascendencia como la conducción de las operaciones militares en los dominios físicos, dando paso al concepto de operaciones multidominio. Estas operaciones se analizan bajo el prisma de dos factores (Estado Mayor de la Defensa de España, 2020, p. 13), el primero dado por la participación y acciones de actores estatales y no estatales que dan origen al concepto de guerra hibrida; y en segundo lugar la desaparición de los limites o fronteras, en esa conjunción de operaciones no lineales y que operan por debajo del umbral de lo convencional y en una zona gris, permitiendo de esta manera soslayar la utilización de los nuevos dominios no físicos y equipararlos con los tradicionales. Frente a esto se ha convertido en una nueva doctrina militar para el accionar conjunto de las fuerzas armadas y de otras agencias gubernamentales y no gubernamentales.

Estado situacional

Existen dos estructuras que conforman la jefatura de inteligencia en los estados mayores de nivel operacional y que se encuentran respaldadas por la doctrina de carácter conjunto, uno es la jefatura de inteligencia del estado mayor conjunto del comando operacional de las fuerzas armadas de Argentina (Estado Mayor Conjunto de las Fuerzas Armadas, 2007, pp.25-27), el cual no presenta una estructura ni una organización determinada, pero que en la enumeración de sus funciones permite vislumbrar cuál podría ser una orgánica que ejecute el proceso de producción de inteligencia. Las funciones que refiere a esta organización poseen una característica extremadamente básica y esencial que comprende las disciplinas tradicionales de Inteligencia y que permite analizar conflictos convencionales y de tercera generación, permitiendo solo actuar en los dominios físicos terrestres, marítimos y aéreos. La segunda jefatura de inteligencia que está establecida en la doctrina conjunta es la del estado mayor conjunto de un teatro de operaciones (Estado Mayor Conjunto de las Fuerzas Armadas, 2018, pp.21-23), la misma está constituida por un departamento de inteligencia y un departamento de medidas de seguridad de contrainteligencia, pero que al igual que la jefatura de inteligencia del comando operacional sus funciones no abarcan las disciplinas de inteligencia necesaria para efectuar el proceso correspondiente que permita asesorar o asistir al comandante

de un teatro de operaciones que desarrolle operaciones militares en un conflicto que abarque tanto los dominios físicos como los no físicos, sean estos en el ciberespacio o actuando en el dominio de la información.

La legislación de las fuerzas armadas argentinas en la ley de reestructuración de las fuerzas armadas (Ley Nro. 24948, 1998, título II) prevé la conformación de un comando operacional, y a su vez dividir el territorio nacional en áreas estratégicas dotadas de comandos de carácter conjunto y con previsiones del nivel estratégico operacional, asimismo la reglamentación de esta ley (Decreto 1691/06, 2006, anexo 1) determina que hasta tanto lo establezca el planeamiento estratégico operacional y no se considere lo contrario, el comando operacional asumirá las tareas como el único comando estratégico operacional, considerando en este sentido al territorio nacional como una única área estratégica para los fines considerados.

En cuanto al empleo del instrumento militar conjunto en el planeamiento y ejecución de operaciones en el multidominio, claramente se distingue el vacío de información, doctrina y lecciones aprendidas de los dominios clasificados como no físicos. En relación a las operaciones en el ciberespacio en el ámbito nacional, la Directiva de Política de Defensa Nacional (Decreto 2645/14, 2014, punto 9),establece riesgos que constituyen situaciones que, de configurarse, podrían afectar los intereses nacionales en materia defensa, uno de estos en particular, es el empleo del ciberespacio con fines militares, incorporándolo como un nuevo ámbito de interés y consolidándolo como un nuevo ambiente operacional, el cual a diferencia de los tradicionales, no posee límites definidos y abarca a los otros factores, es transversal y se superpone sobre ellos, es virtual y no reconoce fronteras locales o interestatales, configura una amenaza a los intereses estratégicos operacionales, afectando la infraestructura estratégica de la defensa. Esto, influenciado por la evolución de las tecnologías y la extensión en forma global de la conectividad, convierten al mismo en un ámbito en el que los estados realizan acciones ofensivas y de influencia en la población, con el objetivo de ganar la mente, el corazón de estos y atraerlos a su causa, generando focos de poder dentro de los países afectados, configurando así lo que se denomina el quinto dominio que es el de la información. Es por ello que las organizaciones militares deben adecuarse a estas nuevas tendencias para minimizar el impacto de estos nuevos riesgos.

Cabe aclarar que ante la inexistencia del elemento de Inteligencia en apoyo al nivel operacional, existe un trabajo final de licenciatura que presenta el diseño de un centro integrador de inteligencia conjunto en apoyo al órgano de dirección de inteligen-

cia de un comando del teatro de operaciones (Sponer, 2012), el cual no será analizado o refutado, y si va a ser tenido en cuenta en el diseño.

Por último y en función de lo descripto hasta el momento es menester presentar el interrogante y dar solución al problema, por lo que ¿cuál debe ser la organización de la jefatura de inteligencia para proporcionar el asesoramiento y la asistencia necesaria al comando operacional de las fuerzas armadas argentinas en el desarrollo de las operaciones multidominio?

Alcances y limitaciones.

El presente trabajo tendrá un alcance circunscripto al campo de la conducción de inteligencia en un estado mayor de nivel estratégico operacional, esta investigación esta apuntada a la conformación de un comando operacional que conduce operaciones en tiempo de paz y hasta tanto se conforme uno o más teatro de operaciones para el caso de operaciones militares durante un conflicto bélico. Asimismo como deberá estar conformada una jefatura de inteligencia de un comando conjunto de un teatro de operaciones.

En segundo término, el trabajo se limitara al análisis de las operaciones de dominio no físico. En primer lugar, el dominio dentro de las operaciones en el ciberespacio, pero apuntadas a la ciberdefensa en el estado argentino y en segundo lugar se limitara a las operaciones de información como quinto dominio, en aquellas que se vean reflejadas a partir del empleo de la tecnología cibernética y el uso del ciberespacio y las redes sociales de características horizontales y de contenido compartido. Además se tendrá en cuenta elementos de la ciberdefensa para la relación con el campo de la conducción, como es el comando conjunto de ciberdefensa, pero que este último no va a ser motivo de análisis.

En tercer lugar se analizara la doctrina extranjera de las fuerzas armadas de España, particularmente la constitución y funcionamiento del centro de inteligencia de las fuerzas armadas (CIFAS).

Por último se abordara como debe ser efectuado el proceso de producción de inteligencia empleando la totalidad de las disciplinas de inteligencia, en los dominios terrestres, aéreos y marítimos, y como los dominios no físicos actúan transversalmente sobre estos.

Teniendo en cuenta que los dominios no físicos comenzaron a tener preponderancia en un mismo nivel que los dominios físicos, el periodo temporal que se va a analizar es desde el año 2007.

Aportes teóricos y/o prácticos al campo disciplinar.

Este trabajo busca aportar un modelo de diseño para estructurar una jefatura de inteligencia en el nivel estratégico operacional, que demuestre como debe estar constituido el órgano de dirección de inteligencia tanto en el comando operacional de las fuerzas armadas, el cual desarrolla actividades y operaciones en tiempo de paz, pero que además sirva de base para estructurar la jefatura de inteligencia conjunta que conformara el estado mayor coordinador del comando de un teatro de operaciones.

Estas estructuras deberán estar compuestas por las diferentes disciplinas de inteligencias que permitan abordar los diferentes dominios físicos y no físicos, para permitir que comandante operacional tome decisiones y el instrumento militar pueda reaccionar frente a operaciones militares del oponente que exceden el ámbito terrestre, aéreo y naval.

Proporcionar una contribución a la doctrina, acerca de la conformación de uno de los campos de la conducción en los estados mayores del nivel estratégico operacional.

Objetivos

Como objetivo general se busca determinar cuál es la estructura orgánica de la jefatura de inteligencia del comando operacional de las fuerzas armadas argentinas que proporcionen el apoyo a la toma de decisiones durante el desarrollo de las operaciones multidominio**.**

Como objetivos particulares se buscara en primer lugar analizar la doctrina vigente de Argentina y España sobre operaciones en el multidominio, que permitan establecer el marco legal para las fuerzas armadas argentinas y analizar la de las fuerzas armadas españolas. En segundo lugar describir las disciplinas de inteligencia que conforman la jefatura de inteligencia en las operaciones multidominio. Y en tercer lugar establecer la orgánica de la jefatura de inteligencia del comando operacional, que facilite la producción de inteligencia, fundamentalmente para los dominios del ciberespacio y el cognitivo.

Hipótesis

La jefatura de inteligencia de un comando operacional organizada con la totalidad de las disciplinas de inteligencia, permitirán el asesoramiento y la asistencia necesaria y suficiente para la toma de decisiones en la conducción de operaciones militares en ambientes de multidominio.

Metodología de la investigación

La investigación se servirá sobre el método deductivo. Asimismo se agregará cierto empleo de inferencias inductivas, debido a que existirá una comparación de diseños de elementos que constituyen la doctrina de los dominios no físicos de las fuerzas armadas de España. En primer lugar se buscara analizar las bases legales de la Argentina que permita delimitar cual es marco de investigación para cumplir con el objetivo. Luego y en la segunda etapa se realizara un compendio de información sobre las operaciones multidominio en las fuerzas armadas españolas y las disciplinas de inteligencias que emplean las fuerzas conjuntas de España y Estados Unidos. La tercera etapa, una vez analizada la información, consistirá en relacionar el sistema de inteligencia estratégico operacional con las operaciones multidominio y posteriormente determinar el diseño de la jefatura de inteligencia.

Se planteará un objetivo general y tres objetivos particulares, de los cuales se desarrollaran conclusiones parciales para dar respuesta a cada uno de los objetivos particulares, posteriormente se elaboraran las conclusiones finales, las cuales brindarán las respuestas al objetivo general planteado en la presente investigación.

Además el diseño de la investigación será de carácter explicativo, en el cual se empleará como técnica de validación el análisis bibliográfico.

Capítulo 1
DOCTRINA Y BASES LEGALES RELACIONADAS AL MULTIDOMINIO.

El presente capitulo tiene por objetivo particular analizar la doctrina y las bases legales de Argentina y aquella doctrina de España sobre las operaciones multidominio. A partir de este objetivo el capítulo permitirá frente a la ausencia de doctrina acerca de las operaciones multidominio en la Argentina, particularmente sobre los dominios considerados no físicos, describir, referir y contextualizar las bases legales y doctrinarias que permiten demostrar la necesidad de organizar un jefatura de inteligencia de un estado mayor conjunto y cuáles son los limites en cuanto a su orgánica y funcionamiento en el nivel operacional conjunto.

Asimismo permitirá analizar aspectos de la doctrina de las fuerzas armadas de España, acerca de cómo llevan a cabo las operaciones multidominio, fundamentalmente en el dominio cognitivo y del ciberespacio. Pero además, porque este país concibe todas sus operaciones, como así también su estructura de mando de manera eminentemente conjunta, teniendo una vasta experiencia en acciones de inteligencia estratégico operacional conjunta.

Sección I
Marco Legal vigente de Argentina.

El Marco legal vigente permite describir cual es el aval necesario que sustente la organización de inteligencia a desarrollar y el elemento de las fuerzas conjuntas multidominio al que deberá proporcionar asesoramiento y asistencia.

> **Ley de Defensa Nacional.** Establece en el artículo 21 que:
>
> Las Fuerzas Armadas estarán constituidas por el Ejército Argentino, la Armada de la República Argentina y la Fuerza Aérea Argentina. Su composición, dimensión y despliegue derivarán del planeamiento militar conjunto. Su organización y funcionamiento se inspirarán en criterios de organización y eficiencia conjunta, unificándose las funciones, actividades y servicios cuya naturaleza no sea específica de una sola fuerza (República Argentina, 1988).
>
> Además expresa en el artículo 22, que:
>
> Los componentes del Ejército, de la Armada y de la Fuerza Aérea de la República Argentina, se mantendrán integrando sus respectivos agrupamientos adminis-

> trativos, dependiendo de los jefes de los estados mayores generales. Conforme resulte del planeamiento conjunto, se dispondrá la integración de estos componentes o parte de ellos, bajo la dependencia de comando estratégicos operacionales conjuntos, específicos o combinados o comandos territoriales. (República Argentina, 1988).

Decreto del Poder Ejecutivo Nacional Nro. 727/2006. Se enuncia en el artículo 13 que "corresponderá al ministerio de defensa, aprobar la readecuación de las estructuras orgánico-funcionales de las fuerzas armadas" (República Argentina, 2006).

Ley de Inteligencia Nacional Nro. 25520. En el artículo 10 determina la creación de la dirección nacional de inteligencia estratégica militar (DNIEM) que depende del ministro de defensa por lo que tendrá como función la producción de inteligencia estratégica militar. (República Argentina, 2001). Además establece que los organismos de inteligencia de las fuerzas armadas tendrán a su cargo la producción de la inteligencia estratégica operacional y la inteligencia táctica necesarias para el planeamiento y conducción de operaciones militares y de la inteligencia técnica específica. (República Argentina, 2001).

Ley de Reestructuración de las Fuerzas Armadas Nro. 24948. Queda establecido en el artículo 4 que la reestructuración y modernización de las fuerzas armadas, asegurará fundamentalmente entre otras medidas, disponer de comandos y estados mayores capacitados para conducir operaciones, realizar estudios, desarrollar el planeamiento y apoyo a la conducción en los diferentes niveles de la conducción. (República Argentina, 1998)

Decreto 1691/2006 del PEN (Organización y funcionamiento de las FFAA). Se destaca que "hasta tanto el planeamiento estratégico no aconseje lo contrario, el comando operacional asumirá que el territorio nacional conformará una sola área estratégica". (República Argentina, anexo 1, 2006). Además considera que se debe promover las capacidades de integración y coordinación del instrumento militar, dándole prioridad al desarrollo de las capacidades de vigilancia, comando, control, comunicaciones, informática e inteligencia. (República Argentina, anexo 1, 2006).

Resolución del Ministerio de Defensa 381/2006. Cabe destacar que se resuelve en el artículo 11 que:

> Los estados mayores del Ejército, la Armada y la Fuerza Aérea solo podrán realizar inteligencia de nivel estratégico operacional y táctico sobre los componentes geográficos, de transporte, telecomunicaciones y científico-técnico, solamente en los casos que éstos incidan y/o estén relacionados con el accionar militar. (República Argentina, 2006).

Decreto 2645/2014 del PEN (Directiva de Política de Defensa Nacional). Referido a la inteligencia militar se menciona que ministerio de defensa por medio de la DNIEM, continuara orientando, coordinando, dirigiendo, planificando y supervisando las actividades del ciclo de producción de inteligencia que realizan los organismos de inteligencia de las fuerzas armadas tanto en el nivel operacional como en el táctico. (República Argentina, punto 6, 2006). Se reafirma además en la posibilidad que dispondrán los estados mayores generales de las fuerzas armadas para proponer modificaciones y readecuaciones de sus estructuras orgánicas y funcionales, siendo estas aprobadas por el ministerio de defensa, con la finalidad de lograr la máxima capacidad de alistamiento, adiestramiento y sostenimiento. (República Argentina, punto 9, 2006)

Decreto 457/2021 del PEN (Directiva de Política de Defensa Nacional). En el año 2021, a través de un decreto del poder ejecutivo nacional se estableció la directiva de política de defensa nacional, donde determina cuales son los aspectos que se deben analizar con respecto a las operaciones multidominio y cómo debe capacitarse el instrumento militar para actuar en ese ámbito. Además describe el contexto y las herramientas para atender en el dominio del ciberespacio que afecten a las infraestructuras críticas en materia de ciberdefensa.

Permanentemente existe una actualización en el empleo de las tecnologías robóticas, de inteligencia artificial, medios en el ciberespacio y de sensores remotos que con el paso del tiempo y en el corto plazo están siendo perfeccionadas.

Esto ha llevado a las defensas nacionales de distintos países a establecer distintas estrategias en el nivel estratégico militar y operacional para la protección de actitudes ofensivas de diferentes actores.

Estos cambios han producido modificaciones relevantes no solo en los teatros de operaciones y en la profesión militar, sino en la extensión y configuración de los campos de batallas.

La transmisión de datos como sus medios de almacenamiento se ha convertido en recursos invalorables para los distintos estados, inclusive tanto para el sector público como privado, siendo reconocidos por las sociedades como medios o ámbitos estratégicos. Frente a esto es imprescindible disponer y considerar la gestión en el dominio de la ciberdefensa que permita disponer libertad de acción en el uso de la tecnología tanto al nivel operacional, estratégico militar y estratégico nacional.

Es de vital importancia para la defensa de los estados, considerar el alcance de las acciones en el ciberespacio. A partir de esto los estados han debido reorientar los esfuerzos de sus sistemas de defensa, dejando atrás la guerra en los dominios tradicionales y dirigiendo recursos hacia el dominio cibernético, agregando de esta manera como un ámbito más al terrestre, naval y aéreo.

Las actividades de ataques cibernéticos que actúan en el ámbito virtual, tienen su incidencia en el ámbito físico, impactando en las ingenierías, como el control aéreo y terrestre, las infraestructuras críticas, el ámbito energético y de abastecimientos hídricos, en los sistemas de comunicaciones militares y civiles, tanto públicos como privados, como así también en todo sistema de comando control. Para la protección y resilencia de estos elementos físicos que componen los intereses vitales de la nación, deberá preverse sistemas de ciberdefensa que permitan sostener el control, la vigilancia, el reconocimiento y la producción de inteligencia militar estratégica y operacional (Decreto 457/2021, 2021, punto 8) tanto en los dominios físicos y no físicos. Además estos sistemas de protección deberán lograr una disuasión creíble frente a las amenazas contra la defensa nacional.

Las actividades de ciberdefensa deben disminuir los efectos de ataques cibernéticos y lograr la resilencia necesaria que permita que el instrumento militar sea empleado en aquellas operaciones militares que afecten a la defensa nacional.

Responsabilidades de Comando Operacional. El comando operacional es el responsable del empleo de los medios militares y la ejecución de las operaciones, tanto aquellas que establece la misión principal, las misiones complementarias, como otras responsabilidades asignadas por el Presidente de la Nación. Además contribuirá al con-

trol efectivo de los espacios territoriales soberanos de la República Argentina en sus dominios terrestre, marítimo, aeroespacial y del ciberespacio.

Para esto, el comando operacional deberá desarrollar capacidades operacionales de ciberdefensa y aquellas destinadas a la protección de las redes informáticas que forman parte del sistema de defensa nacional. Por lo que, la ciberdefensa debe abarcar como un dominio más que contenga a la estrategia militar y operacional, y otra que desarrolle los componentes tácticos.

El nivel operacional deberá recibir en materia de ciberdefensa por parte de la estrategia militar, materializada en el ministerio de defensa, aspectos como los de contemplar e incluir el desarrollo doctrinario, planeamiento, diseño y elaboración de la política de ciberdefensa en el nuevo "Ciclo de Planeamiento de la Defensa Nacional" (Decreto 457/2021, 2021, punto 8).

Además deberá fortalecer el sistema de ciberdefensa, realizando para ello una efectiva supervisión de los organismos correspondientes del estado mayor conjunto de las fuerzas armadas y de los estados mayores generales de las fuerzas armadas (Decreto 457/2021, 2021, punto 8).

También será fundamental fortalecer los vínculos internacionales, fundamentalmente en la región, para el desarrollo de una capacidad soberana en materia de infraestructura de comunicaciones y ciberdefensa, así como "participar en ámbitos de discusión institucional referidos al derecho internacional aplicado al ciberespacio" (Decreto 457/2021, 2021, punto 8).

En relación al diseño operacional deberá desarrollar el objetivo operacional del sistema de ciberdefensa, consistente en la "observación, vigilancia y control de la actividad que acontece en la infraestructura de tecnología informática de las redes del sistema de defensa nacional y de las infraestructuras de la información que le sean asignadas, con el fin de prevenir y contrarrestar incidentes provenientes del ciberespacio. (Decreto 457/2021, 2021, punto 8)

Estado mayor conjunto de las fuerzas armadas. La defensa de los objetivos de valor estratégico, forma parte del proceso de planificación del estado mayor conjunto de las fuerzas armadas, estos objetivos serán establecidos para la aprobación del ministerio de defensa, los cuales constituyen la lista de intereses vitales a proteger de cualquier agresión.

Unos de los aspectos que favorecen a la protección de las infraestructuras críticas, es a través del despliegue de elementos a lo largo y ancho de las jurisdicciones, permitiendo la disuasión, a través de acciones de guerra cibernética, información, energía dirigida y vehículos no tripulados para su empleo en diferente tipo de operaciones.

Por otra parte el estado mayor conjunto de las fuerzas armadas en el nivel estratégico miliar, deberá "desarrollar e incrementar los subsistemas de comando, control, comunicaciones, computación, inteligencia, interoperabilidad, vigilancia y reconocimiento (C4I2VR) (Decreto 457/2021, 2006, punto 9), incorporando capacidades de inteligencia artificial y fundamentalmente este subsistema de comando y control debe estar estructurado para gestionar la acción militar conjunta en el multidominio fundamentalmente en los ámbitos ciberespaciales y dominio de la información o cognitivo.

Por último, en cuanto a la inteligencia militar, el estado mayor conjunto de las fuerzas armadas deberá hacer cumplir con las normativas vigentes, tanto en su nivel como en el estratégico operacional y táctico. Consolidando los sistemas de inteligencia, vigilancia y reconocimientos, en la totalidad de los ámbitos o dominios.

Sección II

Doctrina sobre multidominio de España.

Análisis de la doctrina de inteligencia militar especifica internacional. El desarrollo de la doctrina internacional, permite en primer lugar mostrar la génesis de nuestra doctrina actual, pero además las necesidades de seguir evolucionando sobre la misma, de manera de permitir un apoyo de inteligencia lo más integro posible en cuanto a las explotación de diferentes fuentes de información, en segundo lugar argumentar acerca del diseño de la organización de Inteligencia.

Las fuerzas armadas de España están en una permanente actualización como parte de la OTAN, donde, producto de los avances tecnológicos estos cambios son cada vez más frecuentes, lo que dificulta mantener un modelo permanente. Es aquí donde el entorno operativo lo define la publicación doctrinal conjunta para el empleo de las fuerzas armadas, como el "conjunto de condiciones, circunstancias e influencias que afectan al empleo de las capacidades y a la toma de decisiones, en relación con la operación" (Ministerio de Defensa de España, 2018, p.78)

Es por ello que las fuerzas armadas españolas deben prepararse para enfrentar a todo tipo de oponente que actué con distintos grados de intensidad, es aquí, que las

mismas consideran un entorno operativo a mediano plazo en el cual se expongan estrategias no convencionales que desestabilicen o afecten sus intereses vitales.

Las fuerzas armadas españolas poseen una amplia experiencia en operaciones conjuntas que han sido desarrolladas en los dominios físicos terrestres, marítimos y aéreos. Sin embargo la evolución de su doctrina, esta apuntada a que los dominios no tangibles como el ciberespacio y de información, tengan un mayor protagonismo en el corto plazo al igual que los dominios físicos. Es por ello que las fuerzas conjuntas deben estar capacitadas para actuar en todos los ámbitos de manera de obtener o defender los objetivos operacionales.

Dominio cognitivo.

Delimitación y definición del dominio cognitivo. La desinformación y la propaganda han sido utilizadas históricamente en los conflictos, sin duda que los medios tecnológicos potenciaron su difusión durante el siglo XX. Estas en los preludios de la segunda guerra mundial fueron mutando hacia lo que se conoce como operaciones psicológicas que coadyuvaron a las operaciones militares.

Finalizada la guerra fría, el avance vertiginoso, de teléfonos, internet, teléfonos inteligentes y redes sociales, convirtió a cada persona en una conexión al mundo, lo que permitió la manipulación de la información de manera exponencial, a lo que los estados de occidente advirtieron de manera tardía. Sin duda que la información era una factor importante que afecto o afecta desde las dos guerras mundiales en adelante, pero se consideró que esa información insidia sobre los subsistemas de comando y control y sobre la racionalidad limitada de los lideres a la hora de tomar decisiones. A partir de esa evolución de la tecnología, esta información afecto a las tropas en el campo de batalla, es por ello que los estados mayores comenzaron a considerarlos como operaciones de información.

La fuerzas españolas comenzaron a tomar conciencia de la radicalización de ideas de algunos estados o actores, luego del 11S, cuando tomaron nota de la utilización de medios de transmisión, es aquí donde tuvo preponderancia el concepto de batalla narrativa (Academia de las Ciencias y las Artes Militares, 2020, p.2). Además acciones como las que realizo Rusia sobre Estonia en el año 2007, terminaron de vislumbrar que los países de oriente llevaban una ventaja en estos dominios intangibles.

A partir de esto la doctrina debió adecuarse, fundamentalmente por las experiencias de aquellos estados integrantes de la OTAN que habían obtenidos pobres resultados en los conflictos de Iraq y Afganistán. Esto derivo en un cambio de paradigma en los escenarios del conflicto que pasaron de aquellos terrestre, marítimos y aeroespaciales a dominios muchos más complejos que generaron la necesidad de coordinar los distintos multidominios.

La operación en los diferentes multidominios requiere personal especializados en todos los dominios, esto demuestra que las operaciones de fuerzas armadas llevadas a cabo en los dominios específicos aislados y tradicionales no llevan a una victoria.

Sin duda que resulta ambicioso hoy en día pensar en operaciones multidominio, cuando las acciones conjuntas en lo que refiere a las funciones de comando y control son difíciles de llevar a cabo con total compatibilidad, pero esto impide avanzar en la capacitación para la toma de decisiones y en el accionar de todos los campos de la conducción para las operaciones multidominio.

Claramente la doctrina española conjunta define al dominio cognitivo como aquel que incluye las percepciones, creencias, comportamientos y toma de decisiones de los seres humanos, y la influencia externa que se puede ejercer sobre estos aspectos para modificarlos (Academia de las Ciencias y las Artes Militares, 2020, p.3). Este concepto tiene en cuenta a la persona como un ente individuo y a la vez actuando en una sociedad, es por ello que el dominio cognitivo se consigue o se protege de la gestión de información que las sociedades y el individuo recibe.

La problemática de las Operaciones militares en el Dominio Cognitivo. Es necesario entender que los verdaderos problemas no están a la hora de definir o referir al dominio cognitivo, sino como el dominio de la información se inserta en las operaciones militares, es allí que la mayoría de las operaciones de información o desinformación no surgen en el nivel estratégico militar ni operacional, incluso no tienen como blanco las fuerzas militares, sino que están dirigidas sobre la población que se encuentra presente en el conflicto o más aun sobre los civiles que tienen una relación directa con aquellos que combaten en los campo de batalla. Asimismo y al igual que las ciberoperaciones son muy difícil de determinar su origen, por ende no se sabe hacia dónde dirigir la protección.

Claramente que las operaciones de informaciones en el dominio cognitivo forman parte del concepto de guerra hibrida, tampoco cabe duda que sin estas operaciones

o de la protección frente a estas operaciones es muy difícil lograr estados finales deseados en los conflictos del siglo XXI.

Es relevante destacar que las líneas que separan lo civil de lo militar, como la defensa de la seguridad, cada vez está más difuminado en sus límites, pero que en relación con las fuerzas armadas de la Argentina como estado tiene claramente marcada su diferencia con la seguridad interior, es por eso que debe estar preparada para defenderse de aquellos estados que llevan adelante estas operaciones

Los elementos militares que se utilizan en los dominios clásicos siguen vigente a la hora de actuar en operaciones de información, desinformación y psicológicas, estos son operados por medios operacionales y tácticos siendo apuntados hacia fuerzas oponentes. Es aquí donde las estructuras de mandos se encuentran o deben estar capacitadas en sus estados mayores para realizar estas operaciones y fundamentalmente tener el enlace suficiente con el nivel estratégico nacional, debido a las implicancias políticas que tienen las operaciones.

Es por lo anterior que el dominio cognitivo tiene una relación entre función de combate y campo de la conducción, gestionado por un departamento particular o especial.

Cabe resaltar que la mejor manera desde el punto de vista militar para contrarrestar la desinformación, no es la búsqueda de nodos y noticias falsas, sino a través de una política de comunicación pública que garantice la credibilidad de los mensajes.

Dominio del ciberespacio.

La vertiginosa evolución tecnológica permitió encuadrar al ciberespacio como un factor elemental, pero que no que se lo asociaba o relacionaba a los dominios físicos tradicionales, claramente su relevancia y su influencia en la globalización iniciada fundamentalmente en el este de europa, permitió que este fuese considerado como uno de los cinco dominios a integrar las operaciones multidominio.

Ante esto, la doctrina española considera al ciberespacio como un dominio global, dentro de un difuso entorno de la información, definido en algunas publicaciones como el conjunto de individuos, organizaciones y sistemas que recopilan, procesan, distribuyen o actúan sobre la información (Academia de las Ciencias y las Artes Militares, 2020, p.4). Asimismo, se establece que el espectro electromagnético trasciende tanto los dominios físicos como el entorno de la información.

Las fuerzas armadas de España consideran relevante seguir evolucionando en los estudios innovadores con el ciberespacio y su relación con sus aliados y el mundo académico. En el nivel estratégico operacional es fundamental encontrar un camino que coordine los esfuerzos de todos los dominios tanto físicos como intangibles, sin duda que la respuesta está dada en avanzar hacia los sistemas de comando y control multidominio, que permitan sincronizar y armonizar los esfuerzos específicos de cada componente.

Batalla multidominio.

El concepto de batalla multidominio permite detallar los problemas de tal manera que puedan desarrollarse, aplicarse, comprobar y evaluar las soluciones. Por lo que es importante la determinación de marco del campo de batalla, que permite a los diferentes comandantes específicos y conjuntos visualizar, describir, dirigir, liderar y evaluar el uso del poder de combate en un determinado tiempo, espacio y con los recursos necesarios (Perkins, 2018, p.48).

El concepto de batalla aeroterrestre, que aún se utiliza en las fuerzas armadas argentinas, da un marco de batalla sobre los conceptos de profundo, cercano y de retaguardia, y de cómo las fuerzas armadas en la actualidad puedan lograr una victoria en condiciones de inferioridad, acudiendo a una correcta maniobra operacional. A diferencia de esto, el marco de batalla en las operaciones multidominio debe permitir la victoria no solo en un ambiente complejo, sino que además en ambientes muchos más extensos, abarcando transversalmente desde el campo de batalla hasta las propias unidades con sus asientos de paz, obviamente sin dejar de lado la totalidad del frente y profundidad de las capacidades del oponente.

Se considera fundamental en el análisis de los dominios intangibles que esos lugares virtuales que se abarcan el marco del campo de batalla estén integrados a lugares físicos para establecer una posición de relatividad.

En muchas oportunidades se considera al ciberespacio y al dominio cognitivo netamente virtuales, pero su atribución es incorrecta, porque necesariamente se lo debe considerar sobre un elemento físico de manera de poder incidir con diferentes medios para lograr un efecto. Un ejemplo es cuando un elemento de ciberataque actúa sobre los sistemas de apoyo de fuegos y sistemas antiaéreos, operando desde fuera del teatro de operaciones, como así también estos hackers pueden actuar sobre las familias de aquellos combatientes que se encuentran en el campo de batalla, a través de la utilización de

redes sociales, imágenes o el solo hecho de afectar cuentas bancarias de aquellos que están involucrados en el conflictos.

La Batalla Multidominio, ¿Espacios amplios o comprimidos? La ampliación de lo que se denomina el marco del campo de batalla, a lo que la inteligencia Argentina, define como zona de Interés y zona de responsabilidad, ha sufrido modificaciones en los conflictos modernos, el empleo de los medios físicos cada vez es más acotados a la hora del enfrentamiento aeroterrestre, pero las operaciones de información, las ciberoperaciones y las acciones de guerra electrónica, que demuestran tener un gran alcance, producen una dicotomía entre sí ¿Los campos de batalla han sido comprimidos o ampliados? sin duda que al actuar cualquier fuerza conjunta en operaciones multidominio el espacio, zona u área se convierte en un concepto que no tiene límites geográficos.

Conclusiones parciales.

Teniendo en cuenta las bases legales de Argentina, que ponen en contexto, limitan y encapsulan al nivel estratégico operacional, tanto en su accionar frente a determinados oponentes o las actividades de inteligencia a realizar, se concluye que pese a estas circunstancias las fuerzas armadas argentinas continuaran operando en ámbitos donde existan acciones cibernéticas o de desinformación que afectaran a los elementos que se encuentran conducidos por el comando operacional. Es por ello que el estado mayor conjunto y el comandante operacional deben poseer las capacidades necesarias para protegerse y disponer de los elementos para la forencia y la resilencia suficiente en las operaciones multidominio, fundamentalmente en los dominios cognitivos y ciberespacio.

Capítulo 2
DISCIPLINAS DE INTELIGENCIA PARA EL MULTIDOMINIO.

El presente capitulo tiene como finalidad describir las disciplinas de inteligencia que conforman la jefatura de inteligencia en las operaciones mutidominio. Este objetivo permitirá desarrollar estas disciplinas que reúnen la información sin excluir ningún tipo de dato. Además permite desarrollar cual será la conjunción de fuentes, medios y procedimientos por los cuales se colectara la información para la producción de inteligencia. Asimismo se establecerán aquellas disciplinas que permitan el procesamiento de información y la actuación en los dominios cognitivos y del ciberespacio.

Inteligencia para la acción militar conjunta.

Habíamos descripto anteriormente la existencia y responsabilidades de la DNIEM, quien desde el punto de vista del ciclo de producción de Inteligencia, establece el paso de dirección del esfuerzo de obtención, de acuerdo a los establecido en la doctrina conjunta "guía de planificación de las actividades de inteligencia a través de la cual impartirá los lineamientos específicos que orientarán la planificación y la producción de inteligencia de los organismos de inteligencia de las fuerzas armadas". (Estado Mayor Conjunto de la Fuerzas Armadas, p. 6, 2007).

El sistema de Inteligencia para la defensa, está compuesto, por organismos de inteligencia de las fuerzas armadas y con la jefatura de inteligencia del estado mayor conjunto de las fuerzas armadas, asimismo dentro de cada fuerza armada, el sistema de inteligencia se materializa a través de los distintos canales que existe entre los organismos de inteligencia en los distintos niveles de comando.

En cuanto a la inteligencia de nivel operacional y su relación con la investigación, la doctrina destaca que "la producción de inteligencia estratégica operacional será una responsabilidad de los comandos estratégicos operacionales conjuntos o específicos" (Estado Mayor Conjunto de la Fuerzas Armadas, p. 11, 2007), pero además es muy importante recalcar, lo que describe en cuanto a la disponibilidad que tendrán los comandos operacionales de contar con los medios de ejecución de inteligencia especifico de cada fuerza, "Los comandos estratégicos operacionales planificarán, dirigirán y ejecutarán su propio esfuerzo de inteligencia, contando para ello con los medios idóneos de cada fuerza puestos a su disposición". (Estado Mayor Conjunto de la Fuerzas Armadas, p. 11, 2007)

Áreas de inteligencia. Otro tipo de clasificación que emplea la producción de inteligencia, es el referido a las áreas de inteligencia, siendo aquellas a las cuales el campo de inteligencia distingue por ser de distinta naturaleza, abarcando según las actividades que implican, el lugar, la oportunidad de ejecución y los objetivos sobre los que se ejecutarán. Estas son, el área de proyección que comprende la obtención de información y producción de inteligencia, en todo tiempo, que se proyectarán sobre el componente militar y otros componentes que guarden relación con el poder o potencial militar de los países de interés y el ambiente geográfico bajo control de este, necesarios para el planeamiento de las operaciones futuras. (Ejército Argentino, p.2-8, 2015)

El área territorial que comprende la obtención de información y producción de inteligencia, en todo tiempo, sobre el ambiente geográfico de interés bajo control propio, necesaria para el planeamiento y ejecución de las operaciones militares. Asimismo, la aplicación de medidas de seguridad de contrainteligencia (MSCI), en todo tiempo, necesarias para impedir o neutralizar la actividad de inteligencia por parte de personas u organizaciones reales y/o potenciales que afecten la seguridad de la propia fuerza. (Ejército Argentino, p.2-8, 2015)

Por último, el área de combate que abarca la obtención de información y la producción de inteligencia, durante las operaciones militares, sobre el enemigo real y sobre el ambiente geográfico de la zona de interés, necesaria para el planeamiento y ejecución de operaciones militares. (Ejército Argentino, p.2-8, 2015).

Claramente las áreas de proyección y territorial tendrán mayor énfasis sobre el comando estratégico operacional y el área combate lo tendrá sobre un comando conjunto en un teatro de operaciones.

Estas áreas junto con las disciplinas de inteligencia y los medios de inteligencia, compondrán los diferentes sistemas y subsistemas que proporcionen el apoyo necesario, en este caso al comando operacional de las fuerzas armadas, como así también a los comandos conjuntos estratégicos operacionales.

También conforma el campo de inteligencia, las MSCI siendo estas una parte importante e inseparable de la actividad de inteligencia y están destinadas a "negar información al enemigo y proteger información, documentada o no, materiales, instalaciones, actividades, comunicaciones y personal, de las actividades de inteligencia que pueda realizar el enemigo". (Estado Mayor Conjunto de la Fuerzas Armadas, p. 14, 2007).

Las disciplinas de inteligencia.

Las disciplinas de inteligencia son una guía que permiten no solo orientar la búsqueda, obtención y reunión de información, sino que además permite asegurarle a la producción de inteligencia que no ha sido desechado ningún tipo de información, y a su vez direcciona a los medios de obtención y a los procesos de análisis de la información. Las siguientes disciplinas de inteligencias abarcan todo el espectro de información e inclusive los dominios intangibles, que es hacia donde se dirige la investigación. Hoy las jefaturas, departamentos y divisiones de inteligencia de los diferentes estados mayores específicos y conjuntos basan su estructura en atender a los dominios terrestres, marítimos y aéreos, pero sin duda que la estructura basada en disciplinas de inteligencia permitirá abarcar los ámbitos del multidominio.

Las disciplinas que emplean las fuerzas armadas argentinas poseen la misma característica que las disciplinas que emplean países como España y Estados Unidos. La siguiente clasificación, que si bien es del ejército de los Estados Unidos reúne las mismas características para ser empleadas a nivel conjunto en cualquier fuerza armada, como es la de Argentina.

Inteligencia humana (HUMINT). Recopilación, por un recopilador de inteligencia humana capacitado, de información extranjera, de personas y multimedia para identificar elementos, intenciones, composición, fuerza, disposiciones, tácticas, equipamiento, personal y capacidades. Utiliza fuentes humanas y una variedad de métodos de recolección, tanto pasivamente como activamente, para recopilar información para satisfacer los requisitos de inteligencia del comandante y realizar pistas cruzadas disciplinas de inteligencia. (Ejército de los Estados Unidos, p. 1-4, 2010).

Inteligencia geoespacial (GEOINT). La explotación y el análisis de imágenes e información geoespacial para describir, evaluar y representar visualmente características físicas y actividades geográficamente referenciadas en la tierra. La inteligencia geoespacial consta de imágenes, inteligencia de imágenes e información geoespacial. (Ejército de los Estados Unidos, p. 1-4, 2010).

Inteligencia de imágenes (IMINT). Inteligencia derivada de la explotación de imágenes recopiladas por fotografía visual, infrarrojos, láseres, sensores multiespectrales y radar. Estos sensores producen imágenes de objetos de forma óptica, electrónica o

digitalmente en películas, dispositivos de visualización electrónicos u otros medios. (Ejército de los Estados Unidos, p. 1-4, 2010).

Inteligencia de medición y firma (MASINT). Inteligencia derivada técnicamente que detecta, localiza, rastrea, identifica y describe las características específicas de los objetos y fuentes de destinos fijos y dinámicos. Eso también incluye el procesamiento y la explotación adicional de datos derivados de la inteligencia de imágenes y recopilación de inteligencia de señales. (Ejército de los Estados Unidos, p. 1-4, 2010).

Inteligencia de código o fuente abierta (OSINT). Información relevante derivada de la recopilación, el procesamiento y el análisis de la información disponible públicamente en respuesta a los requisitos de inteligencia. (Ejército de los Estados Unidos, p. 1-4, 2010).

Inteligencia de señales (SIGINT). Categoría de inteligencia que comprende individualmente o en combinación todas las comunicaciones de inteligencia, inteligencia electrónica e instrumentación extranjera, señales de inteligencia, sin importar cómo se transmita. La inteligencia de señales se deriva de las señales de comunicaciones, electrónica e instrumentación extranjera. (Ejército de los Estados Unidos, p. 1-4, 2010).

Inteligencia técnica (TECHINT). Inteligencia derivada de la recopilación y análisis de amenazas militares extranjeras, equipos y material asociado con el fin de prevenir sorpresas tecnológicas, evaluando capacidades científicas y técnicas y el desarrollo de contramedidas diseñadas para neutralizar el adversario de ventajas tecnológicas. (Ejército de los Estados Unidos, p. 1-4, 2010).

Contrainteligencia (CI). Contrarresta o neutraliza los esfuerzos de recopilación de inteligencia mediante la recopilación, investigaciones, operaciones, análisis y producción de contrainteligencia, y servicios funcionales y técnicos. La contrainteligencia incluye todas las acciones tomadas para detectar, identificar, explotar y neutralizar la multiplicidad de actividades de inteligencia de amigos, competidores, oponentes, adversarios y enemigos; y es la clave contribuyente de la comunidad de inteligencia para proteger los intereses y las acciones de los EE. UU. (Ejército de los Estados Unidos, p. 1-4, 2010).

Ciberinteligencia (CYBINT): Se utiliza para transmitir la idea de un conocimiento amplio y mejor calificado del real o potencial eventos relacionados con el ciberespacio que pueden poner en peligro una organización militar del Ejército. Esta última disciplina se desarrolla y es especialmente tenida en cuenta en el proceso de recolección de información de la Inteligencia del ejército y los plasma en el manual de planes, requisitos y evaluación de obtención. (Ejército de los Estados Unidos, p. 3-2, 2014).

Cabe aclarar que el nivel estratégico operacional en las fuerzas armadas argentinas, la disciplina es la de medidas de seguridad de contrainteligencia, lo que implica actividades pasivas de protección y seguridad. Asimismo, el único nivel de inteligencia que ejecuta actividades de contrainteligencia es el nivel de la inteligencia estratégica nacional a través de la agencia federal de inteligencia. Asimismo el nivel estratégico operacional explotara los componentes debidamente autorizados como sus bases legales lo determinan.

Conclusiones Parciales

Si bien las áreas de inteligencias son agrupamientos utilizados fundamentalmente por el componente terrestre para delimitar la obtención de información y su procesamiento, un elemento esencial que busca explotar esta investigación es la descripción de las disciplinas de inteligencia que permiten procesar y organizar la información para que el nivel operacional abarque todos aquellos aspectos que son necesarios en el campo de la inteligencia. Un aspecto a resaltar que se concluye como relevante es la disciplina de ciberinteligencia, aquella que va a permitir reunir toda la información que opera en las redes de computadoras y que afecta a la toma de decisiones, cuando son afectados mediante las operaciones de información a través de las redes sociales, o la anulación de los sistemas de comando y control.

Todas las disciplinas claramente reúnen información para todos los componentes, es claro que la inteligencia geoespacial no será la misma para el componente terrestre, aéreo o marítimo, pero que la reunión en la jefatura de inteligencia permitirá adoptar decisiones que empleen unidades de potencia conjuntas.

Capítulo 3
ESTRUCTURA DE LA JEFATURA DE INTELIGENCIA DEL COMANDO OPERACIONAL DE LAS FUERZAS ARMADAS.

El presente capitulo tiene como finalidad el establecer la orgánica de la jefatura de inteligencia del comando operacional de las fuerzas armadas. Para esto se contextualizara a la jefatura de inteligencia del comando operacional en relación a la inteligencia estratégica militar, además se establecerá cual es la misión de la jefatura de inteligencia de acuerdo a la doctrina vigente, determinando nuevas funciones en base a la necesidad de producir la inteligencia necesaria, no solo para los dominios físicos tradicionales sino aquellos intangibles que faciliten la operación en el multidominio. Asimismo se determina la estructura de la jefatura con los departamentos, divisiones y secciones necesarios que conjuguen a las disciplinas y áreas de inteligencia aptas para los ámbitos multidominios.

Inteligencia estratégica militar.

La jefatura de inteligencia del estado mayor conjunto de las fuerzas armadas, tiene como misión orientar y coordinar el esfuerzo de obtención de información de nivel estratégico militar y producir la inteligencia del mencionado nivel a fin de satisfacer las necesidades del planeamiento militar conjunto y de la conducción estratégica, y las necesidades de inteligencia estratégica militar, conforme a los requerimientos que se reciban de la DNIEM (Estado Mayor Conjunto de la Fuerzas Armadas, p. 6, 2007).

Dentro de las funciones de esta jefatura y relación con el nivel estratégico operacional, se destaca las de reunir, evaluar y compatibilizar la inteligencia obtenida y confeccionar las apreciaciones de inteligencia estratégica de nivel conjunto y otros documentos de inteligencia. Diseminar y difundir, a través del sistema de inteligencia militar conjunta la inteligencia estratégica militar, proveniente de la DNIEM, para los comandos estratégicos operacionales. Y mantener los enlaces funcionales con la DNIEM, las jefaturas de inteligencia de los estados mayores generales de las fuerzas y los organismos de inteligencia de los comandos estratégicos operacionales.

Inteligencia estratégica operacional.

La inteligencia estratégica operacional tiene dos aristas, aquella que se encuentra ejecutando en tiempo de paz y que la doctrina del sistema de inteligencia militar conjun-

to a nivel estratégico la establece en los comandos de áreas estrategias, pero que el decreto 1691, establece que el comando operacional asume la función de esos comandos, y la inteligencia estratégica operacional ejecutada por un comando conjunto de un teatro de operaciones.

A continuación se propondrá cual es la estructura que debe tener una jefatura de inteligencia, que permita satisfacer la conducción del nivel operacional en un ambiente multidominio, donde no solo existen los dominios físicos que hemos analizados, si no los dominios de ciberespacio y de información, teniendo en cuenta que el comando operacional y hasta tanto se conforme un teatro de operaciones, el mismo lleva a cabo operaciones que han sido detalladas en la primera parte de la investigación y que, sus medios y recursos humanos se encuentran expuestos a operaciones de ciberataques, como puede ser durante el desarrollo de la campaña antártica o también una operación de desinformación durante la ejecución de una operación de protección civil o el despliegue de apoyo a un acto eleccionario.

Misión de la jefatura de inteligencia del comando operacional de las fuerzas armadas.

Dirigir y coordinar el esfuerza de obtención de información de nivel estratégico operacional conjunto y producir la inteligencia del mencionado nivel a fin de satisfacer las necesidades del planeamiento y conducción de las operaciones militares. (Estado Mayor Conjunto de la Fuerzas Armadas, p.11, 2007)

Funciones de la jefatura de inteligencia del comando operacional.

- Asesorar y asistir al comandante operacional en la elaboración, ejecución y supervisión de planes, programas y directivas relacionadas con las actividades de inteligencia estratégica operacional necesarias para el desarrollo de las operaciones propias de su nivel.
- Orientar y coordinar el esfuerzo de obtención de información del nivel estratégico operacional.
- Reunir y procesar la inteligencia de interés para el planeamiento estratégico operacional conjunto.
- Proporcionar la información o inteligencia estratégica operacional conjunta al nivel estratégico militar.

- Mantener enlace con los sistemas de inteligencia de fuerzas conjuntas o sistema de inteligencia de fuerzas específicas de otros comandos estratégicos operacionales.
- Mantener enlace durante la paz con las jefaturas de inteligencia de los estados mayores generales de las fuerzas armadas.
- Reunir, evaluar y compatibilizar la inteligencia obtenida y confeccionar las apreciaciones de inteligencia estratégica operacional conjunta, los anexos de inteligencia a los planes y órdenes, y otros documentos de inteligencia.
- Diseminar y difundir, a través del sistema de inteligencia de fuerzas conjuntas, inteligencia estratégica operacional conjunta.
- Formular para su aprobación los elementos esenciales de Inteligencia y otros requerimientos de inteligencia, que se planteen en virtud del planeamiento y conducción de las operaciones militares conjuntas.
- Mantener actualizada la situación de inteligencia en los lugares donde fueren desplegadas fuerzas de paz u observadores militares.
- Requerir a la jefatura II – inteligencia del estado mayor conjunto de las fuerzas armadas la información e inteligencia necesaria para el planeamiento del apoyo a las zonas de emergencia y a la conducción de las operaciones de las fuerzas armadas en el marco del sistema federal de emergencia nacional, las organizaciones militares de paz o de otras operaciones.
- Mantener actualizada la base de datos de información necesaria para la ejecución de actividades de apoyo a la comunidad.
- Establecer y mantener los enlaces necesarios para asegurar el flujo de información pertinente y oportuna en caso de emergencias.
- Asistir y asesorar al comando operacional en la elaboración, ejecución y supervisión de planes y directivas de inteligencia necesarias para ese nivel.
- Proporcionar bases para el planeamiento de las operaciones de responsabilidad del comando operacional.
- Formular propuestas de modificación a la doctrina de inteligencia militar conjunta, sobre la base de la experiencia obtenida en las operaciones en las que intervenga o apoye.
- Planear, coordinar y dirigir las actividades relacionadas con las medidas de seguridad de contra inteligencia en el ámbito militar.
- Intervenir en el planeamiento estratégico operacional del comando.

- Determinar, prevenir y disminuir los efectos de las amenazas y ciberataques que se vayan a producir sobre los sistemas de redes de computadoras que afecten la toma de decisiones del nivel estratégico operacional.
- Determinar, prevenir y disminuir los efectos de las amenazas y ataques producidos por las operaciones de información, que afecten a la toma de decisiones del nivel estratégico operacional y a las tropas que se desempeñen en un teatro de operaciones, una zona de emergencia o las que se encuentren en la zona interior.

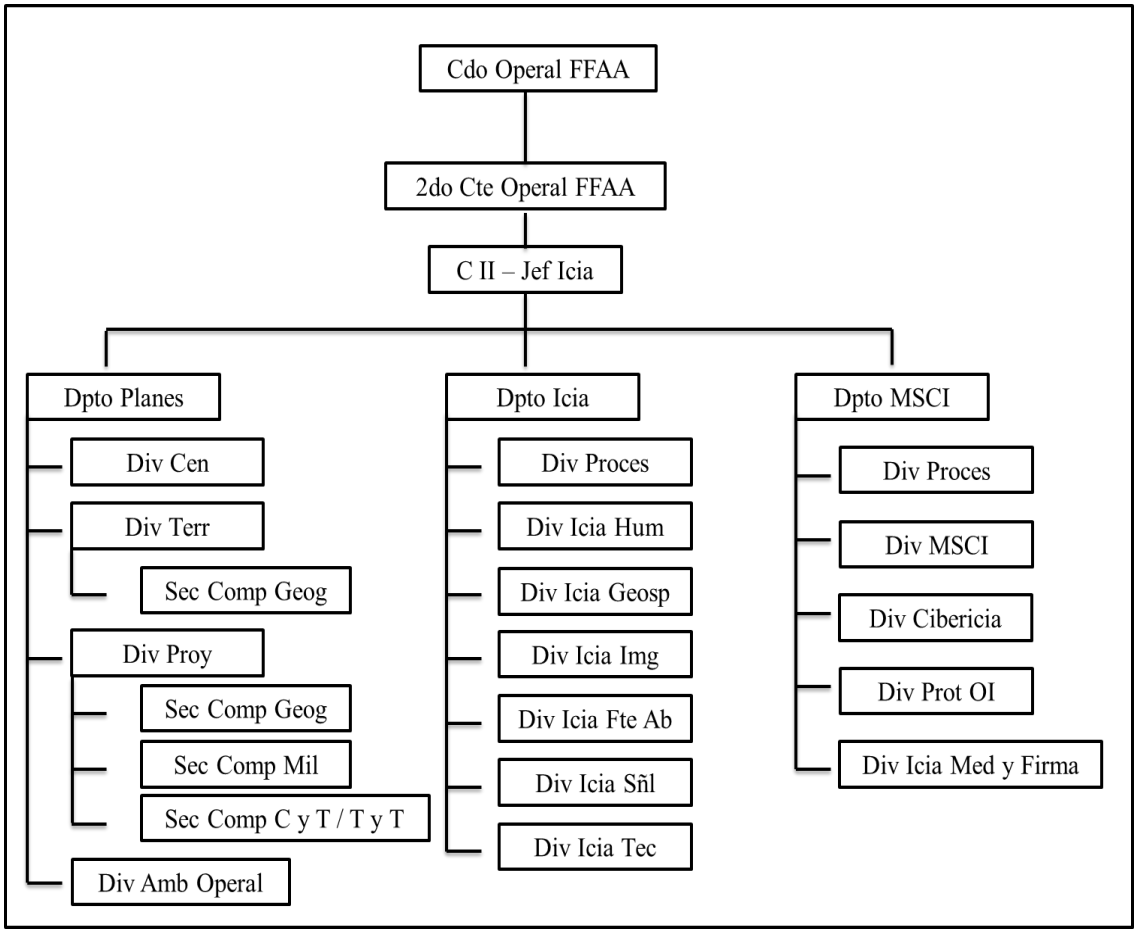

FIGURA 1. Estructura orgánica de la jefatura de inteligencia del comando operacional de las fuerzas armadas para operaciones multidominio.
Fuente: elaboración propia.

Responsabilidades del departamento planes. El departamento planes desarrollara la apreciación de situación de inteligencia estratégica operacional, mediante el procesamiento de la información reunida en los componentes y subcomponentes de la inteligencia estratégica operacional. Además efectuara el análisis del ambiente operacional de interés para las operaciones multidominio.

Las divisiones que integraran el departamento planes es la de central, el de territorial, el de proyección, el de transporte y telecomunicaciones y el de ambiente operacional. Asimismo las secciones serán la de componente geográfico, componente militar, componente científico tecnológico y transporte y telecomunicaciones.

Responsabilidades del departamento de inteligencia. El departamento inteligencia tendrá la responsabilidad de efectuar el procesamiento de la información reunida y su posterior diseminación y difusión, dicha información reunida será registrada, valorizada, analizada, integrada e interpretada, mediante el empleo de las disciplinas de inteligencia humana, geoespacial, de imágenes, de fuentes abiertas, de señales y técnica.

Las divisiones que integraran el departamento inteligencia son las de procesamiento, inteligencia humana, inteligencia geoespacial, inteligencia de imágenes, inteligencia de fuentes abiertas, inteligencia de señales e inteligencia técnica.

Responsabilidades del departamento de medidas de seguridad de contrainteligencia. El departamento de medidas de seguridad de contrainteligencia tendrá la responsabilidad de negar información al oponente y proteger información de las actividades de inteligencia que pueda realizar el oponente, real y/o potencial, mediante la determinación, prevención y disminución de los efectos, amenazas y ciberataques que se vayan a producir sobre los sistemas de redes de computadoras que afecten la toma de decisiones del nivel estratégico operacional. Asimismo deberá determinar, prevenir y disminuir los efectos de las amenazas y ataques producidos por las operaciones de información, que afecten a la toma de decisiones del nivel estratégico operacional y a las tropas que se desempeñen en el teatro de operaciones, zonas de emergencia y en las que se encuentren en la zona interior.

Las divisiones que integran el departamento de medidas de seguridad de contrainteligencia son los de procesamiento, medidas de seguridad de contrainteligencia, ciberinteligencia, inteligencia de medición de firmas, protección de operaciones de información.

Conclusiones parciales.

La constitución de la jefatura de inteligencia de un comando operacional está compuesta por un departamento de inteligencia y un departamento de medidas de seguridad de contrainteligencia que solo dispone de una organización, que puede estar en

capacidad de producir inteligencia en los ámbitos tradicionales, porque los factores del orden de batalla y del ambiente operacional, no consideran aquellos dominios intangibles, asimismo es necesario entender que las estructuras del órgano de dirección de inteligencia deben acatar las limitaciones y restricciones que las bases legales de la Argentina establecen, es por ello que se concluye que la estructura a establecerse será tomando como base las disciplinas de inteligencia distribuidas en los diferentes departamentos y a la luz de las áreas de proyección y territorial, porque el hecho de contemplar todas las disciplinas permitirá reunir procesar toda la información necesaria para el nivel estratégico operacional. Sin duda que la ciberinteligencia y la inteligencia de medición de firmas serán coadyuvantes a la protección de ciberataques y operaciones de desinformación.

CONCLUSIONES FINALES

La presente investigación tuvo por finalidad determinar cuál es la estructura orgánica de la jefatura de inteligencia del comando operacional de las fuerzas armadas argentinas, que logre ser más eficaz para proporcionar el apoyo de inteligencia a la toma de decisiones del comandante operacional durante las operaciones en tiempo de paz y en la responsabilidad de llevar adelante el planeamiento operacional y hasta tanto se conforme un teatro de operaciones. Estas acciones del comando operacional son llevadas a cabo en ambientes de diferente naturaleza a los tradicionales, estos dominios son el ciberespacio y el cognitivo, es por eso, que es menester que la jefatura de inteligencia tenga la capacidad de producir inteligencia en las operaciones multidominio y que su estructura sea acorde.

Para lograr esto, en primer lugar se analizaron aquellas bases legales que permiten darle legitimidad a la estructura de la jefatura de inteligencia, teniendo en cuenta que no existe una doctrina sobre los dominios intangibles. Además se estudió la DPDN vigente, permitiendo conjugar los objetivos que la Argentina persigue en ciberdefensa y multidominios. Posteriormente se efectuó el análisis sobre la doctrina de las fuerzas armadas españolas, referidas a los dominios cognitivos, ciberespacio y las operaciones multidominio en sí, fundamentalmente por la experiencia que ese país posee en el accionar conjunto de sus componentes. Otro concepto de relevancia que se analizo fue el de batalla multidominio pudiendo concluir sobre la amplitud del espacio geográfico que abarcan los dominios intangibles.

En segundo lugar, se realizó la descripción sobre el sistema de inteligencia para la acción militar conjunta, el cual está inmerso el órgano de dirección de inteligencia estratégico operacional, además se analizaron las áreas de inteligencia utilizadas en los diferentes componentes específicos, asimismo se describieron las diferentes disciplinas de inteligencia que son utilizadas tanto en las fuerzas armadas argentinas, como en las de España y los Estados Unidos. Esto permitió concluir que la utilización de todas las disciplinas de inteligencias en cuanto a la reunión y procesamiento de la información permitirán abarcar los diferentes dominios especialmente el ciberespacio y el dominio de la información, teniendo en cuenta los límites que la doctrina y principalmente las bases legales imponen. Es por ello que si bien algunas actividades no está perfectamente autorizadas en el nivel operacional, como es la contrainteligencia, las operaciones de información o las acciones ofensivas de ciberoperaciones, este capítulo permite conocer

el espectro donde se ejecutan estas operaciones y así llevar adelante todas las acciones de protección, prevención, forencia y resilencia frente a estas actividades desarrolladas por estados oponentes.

En tercer lugar, se describió la relación de la inteligencia operacional con la inteligencia estratégica militar y como a través del sistema de inteligencia de fuerzas conjuntas permitirá proporcionar la inteligencia necesaria al comando operacional, a los componentes específicos. Asimismo se analizó la misión y las funciones que el sistema de estratégico operacional establece y sus funciones correspondientes, las cuales no fueron modificadas, pero se concluyó sobre la necesidad de agregar funciones referidas a la protección y disminución de los efectos generados por los ataques o amenazas cibernéticas y operaciones de información. Además se concluyó como debe estar estructurada la jefatura de inteligencia, manteniendo los departamentos tradicionales de inteligencia y medidas de seguridad de contrainteligencia, pero conformada con las disciplinas y áreas necesarias para producir y proporcionar la inteligencia a la toma de decisiones en todos los dominios tangibles e intangibles.

BIBLIOGRAFÍA

Academia de las Ciencias y las Artes Militares (2020). *El dominio cognitivo en las operaciones multidominio.* Madrid, España, junio de 2020.

Academia de las Ciencias y las Artes Militares (2020). *Las Operaciones Multidominio desde la perspectiva de la Alianza Atlántica.* Madrid, España, abril de 2020.

Campos G. (2020). *Inteligencia Estratégica, Aproximación conceptual y metodológica,* ESG. Ciudad de Buenos Aires, Argentina. 2019.

Davidson P., Glass R. (1948). *Inteligencia es para Comandantes.* Empresa de Publicaciones del Servicio Militar. Estados Unidos, 1948.

Ejército Argentino (2015). *Conducción para las Fuerzas Terrestres.* Ciudad de Buenos Aires, Argentina, 2015.

Ejército de los Estados Unidos de América (2014). *Planeamiento y requerimientos en la evaluación de Obtención*. Washington DC, Estados Unidos de América, 19 de agosto de 2014.

Ejército de los Estados Unidos de América (2010). *Manual del Oficial de Inteligencia.* Fort Huachuca, Estados Unidos de América, enero de 2010.

Estado Mayor Conjunto de las Fuerzas Armadas (2020). *Comando Operacional del Estado Mayor Conjunto de las Fuerzas Armadas.* Recuperado de www.fuerzas-armadas.mil.ar/Dependencias-COPERAL.aspx

Estado Mayor Conjunto de las Fuerzas Armadas (2007). *Reglamento Orgánico del Comando Operacional*. Ciudad de Buenos Aires, Argentina, 2007.

Estado Mayor Conjunto de las Fuerzas Armadas (2018). *Estado Mayor Conjunto del Comando de un Teatro de Operaciones.* Ciudad de Buenos Aires, Argentina, 2018.

Estado Mayor Conjunto de las Fuerzas Armadas (2018). *Inteligencia para la Acción Militar Conjunta.* Ciudad de Buenos Aires, Argentina, 2007.

Estado Mayor Conjunto de las Fuerzas Armadas (2018). *Sistema de Inteligencia Militar Conjunto Nivel Estratégico.* Ciudad de Buenos Aires, Argentina, 2007.

Estado Mayor de la Defensa de España (2020). *Nota conceptual Operaciones Multidominio.* Madrid, España, 02 de abril de 2020.

Decreto 1691/06. Organización y funcionamiento de las Fuerzas Armadas (2006). *Boletín Oficial de la República Argentina*, 22 de noviembre de 2006.

Decreto 2645/14. Directiva de Política de Defensa Nacional (2014).*Boletín Oficial de la República Argentina*, 19 de enero de 2015.

Ley Nro. 24948. Ley de Reestructuración de las Fuerzas Armadas, publicada en el *Boletín Oficial de la República Argentina*, 03 de abril de 1998.

Ministerio de Defensa de España (2018). *Doctrina para el empleo de las Fuerzas Armadas.* Madrid, España, 2018.

Perkins D. (2018).*La Batalla Multidominio,* Military Review, Kansas, Estados Unidos, 2018.

Sherman K. (1951).*Inteligencia Estratégica,* Círculo Militar, Vol. 391. Ciudad de Buenos Aires, Argentina, 1951.

Sponer J. (2012).*Diseño de un Centro Integrador de Inteligencia Conjunto en apoyo al C2 de un Comando de Teatro de Operaciones.* Trabajo Final de Licenciatura, ESG, Ciudad de Buenos Aires, Argentina, 18 de setiembre de 2012.