EJÉRCITO DE CHILE
DIVISIÓN EDUCACIÓN
Academia de Guerra

LA CIBERDEFENSA COMO PROBLEMA ESTRATÉGICO

Memoria para obtener el título de Oficial de Estado Mayor del Ejército de Chile

MAYOR FELIPE MIÑO DEICHLER

PROFESOR GUÍA
CORONEL GERMÁN VILLARROEL OPAZO
Oficial de Estado Mayor del Ejército, Magíster en Historia Militar y Estrategia
Magister en Ciencias Políticas de la Pontificia Universidad Católica

Santiago de Chile

2022

A todos ellos que han permitido impulsar mis motivaciones, esos que empatizaron con mis creencias y articularon con su apoyo mi desarrollo personal y académico, eterno agradecimiento a quienes creyeron y no se apartaron de mí.

ÍNDICE

LISTA DE ABREVIATURAS

Abreviaturas	Definición
CCP	Centro Cibernético Policial
CEEAG	Centro de Estudios Estratégicos de la Academia de Guerra
COps	Ciberoperaciones
CCC	Comando Conjunto Cibernético
CONPES	Consejo Nacional de Política Económica y Social
DSCA	Defense Support to Civilean Authorities
DDoS	Denegación de Servicio Distribuida
DoD	Department of Defense
DIME	Diplomático, Informaciones, Militar y Económico
ColCERT	Equipo de Respuestas de Incidentes de Colombia
EMCO	Estado Mayor Conjunto
EMAD	Estado Mayor de la Defensa
FAs	Fuerzas Armadas
GPC	Guía de Planificación del Comandante
IDM	Internal Defense Measures
II/ITSEC	Interservice/Industry Training, Simnulation, and Education Conference
JEMCO	Jefe del Estado Mayor Conjunto
JEMAD	Jefe del Estado Mayor de la Defensa
JIPOE	Joint Intelligence Process of Operational Enviroment
LA	Líneas de Acción
MCCE	Mando Conjunto del Ciberespacio
MILNET	Military Nets
MOD	Ministry of Defense
ORM	Opción de Respuesta Militar
ONU	Organización de las Naciones Unidas
OTAN/NATO	Organización del Tratado del Atlántico Norte
ONGs	Organizaciones No Gubernamentales
PNCD	Política Nacional de Ciberdefensa
PNCS	Política Nacional de Ciberseguridad
PEMSII-PT	Políticas, económicas, militares, sociales, infraestructura, informaciones, tiempo y espacio.

RCDS	Royal College of Defense Studies
SECDEF	Secretary of Defense
UE	Unión Europea
USAF	United State Air Force
USCYBERCOM	United State Cyber Command

TABLAS

FIGURAS

RESUMEN

La presente investigación tiene por propósito determinar cuáles son las implicancias de la *Ciberdefensa*, que determinan su influencia en el nivel estratégico de la conducción militar, enmarcado en la evolución de las operaciones en el ciberespacio hasta el año 2021 (año en que finaliza la investigación). Inicialmente, el trabajo se orientó a la delimitación del concepto *problema estratégico* centrándose en la acepción de estrategia como *nivel de la conducción militar,* a través del análisis de las variables operacionales, políticas, económicas, militares, sociales, información, infraestructura, ambiente físico y tiempo (PEMSII-PT), sin dejar de considerar las implicancias legales asociadas. Por otro lado, la definición de *problema,* asociado a la estructura de un *problema complejo* o más bien en el término acuñado en inglés como *wicked problem* [1] *.* Seguidamente, la investigación buscó determinar cuáles son las características de la *Ciberdefensa* en el contexto del 5to dominio de la guerra, y se analizó el comportamiento de los *Principios de la Guerra* descritos para el nivel conjunto y su aplicabilidad en el ciberespacio. De esta manera se pudo determinar la relación entre ambos y el problema que esto representa para el nivel estratégico de la conducción militar. Finalmente, con estos antecedentes, la investigación permitió establecer los argumentos para afirmar que la *Ciberdefensa* puede y debe abordarse como un problema del nivel estratégico.

Palabras claves: *Ciberespacio – Ciberdefensa – Estrategia – Nivel estratégico – Problema Estratégico*

[1] Wicked Problem, en su traducción directa se entiende como un “problema perverso”, término acuñado para aquellos problemas sin solución o una solución compleja de identificar. Esta conceptualización hace ver la existencia de problemas multifactoriales que se asemejan a la problematización militar del más alto nivel.

ABSTRACT

This research aims to determine the implications of cyber defense, which determine its influence on the strategic level of military leadership, framed in the evolution of operations in cyberspace until the year 2021 (the year in which the research ends). Initially, the work was oriented to the delimitation of the strategic problem concept focusing on the meaning of strategy as a level of military leadership, through the analysis of operational, political, economic, military, social, information, infrastructure, physical environment, and time (PEMSII-PT) variables, without neglecting the associated legal implications. Without a doubt, the problem is embedded in a complex structure - a wicked problem. Next, the research sought to determine the characteristics of cyber defense within the fifth domain of war and the behavior of the principles of war at the joint level to analyze its applicability in cyberspace. This method generated a better understanding of the relationship between cyber defense characteristics and behavior and the strategic-level problem presented to senior military leadership. Finally, with this background, the research allowed us to establish the arguments to affirm that Cyber Defense can and should be approached as a strategic level problem.

Keywords: *Cyber space – Cyber defense – Strategy – Strategic Level – Strategic Problem*.

INTRODUCCIÓN

La apertura de las fronteras a través del ciberespacio ha venido a revolucionar la manera de convivir no solo de las personas, sino que también de los mismos estados en busca de mantener sus intereses y, un nivel de supervivencia que les permita mantener la libertad de acción necesaria para el desarrollo próspero y libre de la nación. Es en ese contexto que, el gobierno de Chile, a través de la Política Nacional de Ciberseguridad (PNCS) ha determinado conceptos y lineamientos claros y, más importante aún, ha definido el marco regulatorio para el desarrollo de una Política Nacional de Ciberdefensa.

Tan solo el hecho de considerar el tratamiento del ciberespacio desde el sector de la Defensa Nacional, hace responsables a las instituciones de las Fuerzas Armadas (FAs) primero; de determinar cuáles son sus responsabilidades y alcances respecto al tema, segundo; de identificar las metas y, tercero; consecuente con lo anterior, visualizar cuáles son las brechas en el desarrollo de capacidades para dar cumplimiento a los objetivos nacionales. En este contexto es que surge la necesidad de establecer el nivel donde debe ser tratada la Ciberdefensa

Conforme a la determinación del *quinto dominio de la guerra*, como se ha denominado al ciberespacio en el ámbito de la Defensa y, a los efectos que pueden llegar a generar las acciones a través de la Ciberdefensa, como una de las opciones de respuesta militar, el propósito de este trabajo de investigación fue entregar los argumentos para identificar cuáles son las características de la Ciberdefensa que la determinan como un problema de la conducción estratégica nacional.

Para lograr el objetivo propuesto, el trabajo se desarrolló en cuatro partes, la primera de ellas fue establecer el marco conceptual en el que iba a ser desarrollada la investigación, realizando precisiones de algunos conceptos nucleares ante la diversidad de posturas respecto a la Ciberdefensa. En este punto se establecieron los parámetros de análisis y los objetivos intermedios que contribuyeron a validar la tesis del trabajo de investigación.

En segundo término, se trabajó sobre la comprensión del concepto de *problema estratégico,* que fue tratado en partes separadas; en primera instancia, para determinar el *problema militar* y posterior a ello el *nivel de la conducción estratégica*, para finalmente dejar establecido por parte del autor el concepto de *problema estratégico*, que serviría como punto

de partida a los objetivos posteriores. Con lo anterior se dio cumplimiento al primer objetivo intermedio que era *distinguir qué es un problema estratégico.*

En tercer lugar, los esfuerzos investigativos estuvieron enfocados en la identificación y descripción de las *características estructurales* de la Ciberdefensa. Dicho concepto, se entendió como todas aquellas definiciones, principios, alcances y encuadramientos en las estructuras gubernamentales de los países de referencia, como así mismo en Chile. Los resultados de esta comparación, y a la luz del concepto de *problema estratégico*, permitieron establecer que en Chile la Ciberdefensa está tratada desde la estructura del Estado Mayor Conjunto, pudiendo a través del cumplimiento de este segundo objetivo, comenzar a tributar al objetivo central de la investigación a partir de la distinción de las características estructurales de la Ciberdefensa.

En cuarto lugar, se logró identificar el comportamiento de la Ciberdefensa a la luz de las variables de análisis estratégicas, y la aplicabilidad de los principios de la guerra en el quinto dominio de la guerra. Para las primeras, se consideraron las variables PEMSII-PT y para el segundo factor, los nueve principios de la guerra establecidos por la Doctrina Nacional Conjunta. El análisis por separado de estos factores permitió dar cumplimiento a los objetivos parciales planteados, y más importante aún, tributar en forma robusta al objetivo principal de la investigación.

Todo lo anterior, además de una exhaustiva revisión bibliográfica tanto de doctrinas nacionales como extranjeras, así como publicaciones y estudios militares afines, lo que también fue confrontado con la experiencia de diferentes especialistas en el ámbito de la conducción estratégica como de la Ciberdefensa, dando así la rigurosidad científica a la investigación.

Por último, y considerando lo anteriormente expuesto, fue factible para el autor establecer conclusiones concretas respecto a cada uno de los objetivos parciales, y más importante aún, comprobar la tesis planteada pudiendo identificar las características de la Ciberdefensa que la determinan como un problema de la conducción estratégica.

CAPÍTULO I
PROBLEMA DE INVESTIGACIÓN

1. Planteamiento del Problema

1.1 Antecedentes del Problema

La posibilidad que ofrece la tecnología para hacer permeable las fronteras físicas y eliminar las distancias, ha entregado nuevas formas de relacionarse entre los estados y las organizaciones, pudiendo ampliar las conexiones en el amplio espectro de lo diplomático, económico, ambiente de información y sin lugar a duda, en el ámbito militar. Es decir, más que simplificar la manera de relacionarse, se ha complejizado, pudiendo afirmar que nuestro entorno es global, con las fortalezas y amenazas asociadas a dicha apertura.

Las políticas de los estados se han ampliado al escenario abstracto del ciberespacio, debiendo preocuparse por la seguridad de los intereses nacionales, así como de las alianzas internacionales, apareciendo en escena la necesidad de la *Ciberseguridad*. El concepto de ciberseguridad[2] es aplicable a la vida cotidiana de las personas como de las organizaciones, tanto en la protección de bases de datos de estamentos privados, como capitales de información de instituciones del Estado; por lo tanto, los impactos que pueden generar las vulneraciones de uno u otro no pueden obedecer a los mismos términos de acción o planificación. El amplio concepto de ciberseguridad se fue haciendo específico, y se manifestó en políticas de guerra, puntualmente c*iberguerra,* y en el caso de Chile en su Política de Defensa Nacional, derivando en el concepto específico de *Ciberdefensa,* plasmado en la "Política Nacional de Ciberdefensa" (Diario Oficial, 2018)

Al respecto, se pudo inferir que, si la *Ciberdefensa* ya se había considerado como una arista necesaria en la evaluación de la seguridad de los intereses del Estado, en el

[2] Ciberseguridad es el "conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan" (Cano, 2013).

más alto nivel de la conducción política, esto consecuentemente deriva en que la *Ciberdefensa* debe ser abordada por el *Nivel Estratégico* de la conducción militar. De esta manera, concebir soluciones pertinentes a este nivel, es decir, definir el qué, dónde y cuándo emplear el poder nacional en el ciberespacio, debiendo prospectar en este ambiente abstracto, cuál es la fuerza que se debe emplear, y cómo usarla para dar cumplimiento a la voluntad política.

En esta línea, el Ministerio de Defensa Nacional de Chile elaboró la Política Nacional de Ciberdefensa, la cual fue concebida como *"la respuesta a los nuevos riesgos y amenazas, que el ciberespacio genera para las capacidades de la Defensa Nacional, las cuales incluyen, entre otros elementos, la información, la infraestructura y las operaciones de defensa"* (Congreso Nacional, 2018: p.3)

De lo anterior, surgió la imperiosa necesidad de definir las características del ciberespacio, determinar la relación que existe con las *variables operacionales*, (PEMSII-PT) por un lado, y por otro la aplicabilidad de los *principios de la guerra* declarados en el nivel de la planificación estratégica nacional en este nuevo escenario.

La definición de las *características estructurales de la Ciberdefensa* y la vinculación con las *variables operacionales*, específicamente para esta investigación las variables; *militar*, *infraestructura* e *informaciones*, y los *principios de la guerra,* permitieron establecer el por qué la *Ciberdefensa* debe ser considerada como un problema del nivel de la conducción estratégica.

1.2 Preguntas de investigación

1.2.1 Pregunta general

¿Por qué la *Ciberdefensa* constituye un problema estratégico en la conducción militar?

1.2.2 Preguntas específicas

1. ¿Qué se entiende por problema estratégico?

2. ¿Cuáles son las características estructurales de la *Ciberdefensa* en el contexto del 5to dominio de la guerra?

3. ¿Cuál es el comportamiento de la Ciberdefensa en el contexto de *variables de análisis estratégicas nacionales*?

4. ¿Cuál es la aplicabilidad de los *principios de la guerra* conjuntos en el Ciberespacio?

1.3 Objetivos

1.3.1 Objetivo general

Determinar las características de la *Ciberdefensa* que la determinan como un problema estratégico para la conducción militar.

1.3.2 Objetivos específicos

1. Distinguir qué es un *problema estratégico.*

2. Describir las características estructurales de la *Ciberdefensa* en el contexto del 5to dominio de la guerra.

3. Identificar cómo se comporta la *Ciberdefensa* en el contexto de las *variables de análisis estratégicas* nacionales*.*

4. Examinar la aplicabilidad de los *principios de la guerra* conjuntos en el *Ciberespacio*.

1.4 Justificación de la investigación

La investigación era necesaria, debido a que no existe un documento o fuente bibliográfica institucional que aúne los conceptos teóricos de la *Ciberdefensa* con los *factores de análisis del nivel estratégico* y la metodología de estudio de la guerra a través de los *principios* que la rigen. La experiencia que existe es que los textos doctrinarios se refieren brevemente al 5to dominio de la guerra[3], abordándolo solo como un elemento más para la comprensión del ambiente operacional. Consecuente con ello, se conceptualiza la *Ciberdefensa* como "*acciones en el marco de la política de ciberseguridad, orientada a proteger el ciberespacio, así como el conjunto de políticas y técnicas de la defensa nacional para enfrentar amenazas y riesgos…"* (Ejército de Chile, 2017:p.137), lo anterior, de repercusiones transversales a todos los niveles de la conducción, orientó a dar respuestas tecnológicas específicas. El resultado del presente trabajo entregó un insumo consistente para el análisis y comprensión del concepto de *Ciberdefensa* que permite comprender las características que la hacen identificable como un problema estratégico. Lo anterior es relevante, ya que se transforma en un aporte teórico aplicable y necesario para considerar como base conceptual para la planificación estratégica relacionada con la Defensa del Estado de Chile.

1.5 Delimitación de la investigación

1.5.1 Temporal

El límite temporal estuvo determinado por el período desde la declaración de uso de Redes Militares (MILNET) en el año 1983 y hasta el año 2021, año en que finalizó la investigación. Lo anterior de manera retrospectiva, estableciendo así, que no existió una intención en la prospección de nuevos escenarios, tendientes a ampliar las

[3] Los dominios de la guerra se entienden como Tierra, Aire, Mar y Espacio y se ha aquilatado como 5to dominio al ciberespacio, considerando qué el ambiente operacional es influenciado por el ambiente de la información.

consideraciones ya existentes referidas al Ciberespacio, *Ciberdefensa* o a nuevas capacidades tecnológicas que vengan a modificar las condiciones vigentes.

1.5.2 Espacial

La investigación se desarrolló en el contexto teórico de las ciencias militares, específicamente en el nivel estratégico de la conducción militar en Chile y conforme a las características estructurales de la teorización de la Ciberdefensa y las características con las puede llegar a afectar el nivel de la conducción en forma específica.

1.5.3 Conceptual

La investigación se limitó a abordar la *Ciberdefensa* en el ámbito conceptual y sus características como fenómeno de la conducción militar, relacionado exclusivamente con las *variables operacionales* (militar – infraestructura – informaciones) y, con los elementos teórico-prácticos de los *principios de la guerra* en el nivel conjunto, buscando determinar las características de la *Ciberdefensa* que la definen como un problema estratégico**.**

1.6 Marco Teórico-Conceptual Referencial

Durante las últimas dos décadas los conceptos de *Ciberespacio, Ciberseguridad, Ciberguerra* y *Ciberdefensa* se han hecho cada vez más comunes en diferentes ámbitos, al punto que la bibliografía disponible es múltiple, sin siquiera haber un consenso respecto a una definición y delimitación de cada uno de ellos. En ese sentido se hizo necesario establecer, no sólo un marco teórico referencial, sino que además la presentación y desarrollo de *conceptos nucleares* (Peñaloza, 2017), que dieron el marco a la investigación para poder determinar las características de la *Ciberdefensa* que la convierten en un problema estratégico.

Para lo anterior, es preciso señalar que el consenso de las definiciones desarrolladas, pivotean sobre la definición de *Ciberdefensa,* de tal manera de delimitar la acción investigativa sobre las características estructurales de ésta. Respecto a la búsqueda de la relación con la estrategia y más específicamente a su determinación como *problema estratégico*, fue necesario también acotar el desarrollo de estos conceptos, centrando todo el esfuerzo sobre la acepción de estrategia como *nivel de la conducción*.

Concordante con lo anterior se seleccionaron factores de análisis para este efecto, por un lado, aquellos estratégicos asociados a las determinantes de un problema en el espectro de las *variables operacionales* (PEMSII-PT), específicamente en lo *militar*, la *infraestructura* y las *informaciones* y, por otro lado, *los principios de la guerra* en el nivel conjunto, manteniendo así un anclaje sobre un factor conocido y permanente en el análisis de esta, yendo en búsqueda de aquellos que fueran identificables en la *Ciberdefensa* dentro del ambiente operacional, y su espacio de batalla, el *ciberespacio*, también aceptado como un dominio más que compone el ambiente operacional, conforme lo define la doctrina nacional. (Ejército de Chile, 2017).

Planteado todo lo anterior, el marco teórico-conceptual fue desarrollado en dos grandes agrupaciones conceptuales, la primera de ellas relacionada con los conceptos de *Ciberespacio, Ciberguerra y Ciberdefensa,* y la segunda asociada a la *estrategia* como nivel de la conducción y la determinación del problema estratégico, así como, las *variables de análisis estratégicas* (militares – infraestructura – informaciones) y los *principios de la guerra*, como ha sido declarado en los párrafos precedentes.

En cuanto al *Ciberespacio***,** como se ha expresado anteriormente, no existe consenso en la definición de este, aun cuando se constata su uso desde la década de los ’80 existiendo elementos comunes que permitieron precisar una definición.

La Política Nacional de Ciberseguridad (2017), el DNC 2-11 Doctrina Conjunta de Ciberdefensa (2018) y el D-10001 “El Ejército” (2017), lo definen como: *"el ambiente intangible compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior"*. Por su parte el Departamento de Defensa de los Estados Unidos (DoD), lo define como “*un*

dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores y controladores". (Roldán, 2013: p.17).

De las definiciones anteriores se pudo colegir que nos enfrentamos a una dimensión que abarca componentes tanto abstractos como físicos, que involucra su uso para fines privados y estatales, lo que consecuentemente lo hace parte del ámbito de acción militar desde el momento en que el *Ciberespacio* contiene en sí, capitales de información[4] e infraestructuras críticas[5] que permiten el desarrollo de la nación, instituciones y personas. Ante la necesidad de requerir el uso seguro del *Ciberespacio,* surgió la responsabilidad de defenderlo ante cualquier acción de ofensa extranjera, o de grupos no estatales. En atención a los intereses radicados en este dominio, se opondrán naturalmente voluntades, al tratar de ser controlado o bien al transformarse en un medio para alcanzar los fines políticos, en el orden de la supervivencia del Estado o supremacía de este en un nivel regional respecto al ambiente de información.

En atención a todo lo anterior, para el presente estudio se entendió el ciberespacio como: *el entorno físico y abstracto que se desenvuelve en el ambiente de la información e involucra las plataformas, capitales de información y las relaciones e interacciones sociales que tienen lugar en este*[6].

Debido a lo expuesto se pudo inferir que el ciberespacio, ya sea en su totalidad o en una parte de sus componentes, es útil para conseguir objetivos nacionales que benefician a todos los ciudadanos y en atención a que este puede ser aprovechado o atacado por otros, debe ser defendido, pudiendo generarse un conflicto denominado *Ciberguerra,* la que tendrá cabida desde el momento en que dos o más voluntades (estados, coaliciones, organizaciones internacionales e incluso personas)

[4] Gestión de datos, información de materias sensibles que involucran la experiencia y capacidades de administración de volúmenes de datos en torno a los cuales gira la información.
[5] Redes de telecomunicaciones, nodos de distribución, medios de propagación que, de ser afectadas o destruidas total o parcialmente, podrían afectar gravemente al normal funcionamiento de una organización o de un Estado.
[6] Definición elaborada por el autor.

se opongan por el dominio de la información contenida en el *Ciberespacio,* o por el control de las relaciones establecidas en él.

En cuanto a la *Ciberguerra,* al igual que en el caso anterior, las definiciones del concepto no han llegado a un punto en común desde donde se pueda establecer una comprensión absoluta de lo que involucra esta. Una definición que contiene elementos a considerar es la que propone Gema Sánchez M. (2009) en la revista Política y Estrategia, entendida como *"una agresión promovida por un Estado y dirigida a dañar gravemente las capacidades de otro para tratar de imponerle la aceptación de un objetivo propio o, simplemente, para sustraerle información, cortar o destruir sus sistemas de comunicación, alterar sus bases de datos, es decir, lo que habitualmente hemos entendido como guerra"* (p. 255). Esta definición señala concretamente la participación de un Estado contra otro, en pos de la imposición de la voluntad, es decir, un modelo de guerra tradicional con dos actores claramente definidos.

Una definición un poco más amplia de *Ciberguerra* es aquella que expone el Tcl. Lionel Alford (2001) en su artículo académico, *"Ciberdefensa, una nueva doctrina y taxonomía"*, de la Fuerza Aérea de los Estados Unidos (USAF), estableciendo que es *"cualquier acto destinado a obligar a un oponente a cumplir con nuestra voluntad, ejecutada contra los procesos de control de software dentro de un sistema de oponentes. Incluye los siguientes modos de ciberataques: infiltración cibernética, manipulación cibernética, asalto cibernético, ciberataques".* Aquí ya no se identifican actores, más bien solo se refiere al fenómeno por medio del cual se impone la voluntad.

Otra manera de interpretarla es aquella planteada por el Crl. José Hidalgo (2014) del Ejército de Tierra de España, quién propone que la *ciberguerra* "*es un nuevo paradigma que adopta elementos de la Guerra Total y la Guerra Asimétrica"* , basado en los argumentos de:

- *"Afecta a todos los ciudadanos, administraciones, instituciones y empresas del Estado" (Guerra Total).*
- *"Relación costo-eficacia es muy alta" (Guerra Asimétrica).*
- *"No necesita de una gran infraestructura militar" (Guerra Asimétrica)* (p. 37).

Por último, fue pertinente considerar otra definición que abarca de una u otra manera a las anteriores, ya que se observan elementos como el Estado, otros actores y donde están en juego objetivos políticos y militares; es la que define la ciberguerra como *"un fenómeno de redes que consiste en la confrontación cibernética de uno o más actores estatales con otros actores similares u otras redes que decidan llevarla a cabo en contra del Estado, cuyo fin es obtener ventajas con procedimientos ofensivos de carácter tecnológico, en el contexto de un conflicto político o militar"* (Lodeiro, 2011: p. 40).

Esta última definición abarca de manera más global el concepto, incluyendo a actores en conflicto, que pueden ser variables, pero manteniendo siempre al Estado como una de las partes enfrentadas y, al ser complementada con la lógica establecida por José Hidalgo, permitió obtener un marco conceptual para la comprensión del término de Ciberguerra.

Habiendo definido el *Ciberespacio* como: *el ambiente físico y abstracto donde se consagran los capitales de información, la infraestructura tecnológica y las relaciones sociales contenidas en las redes*, y la *Ciberguerra* como la posibilidad de que exista un conflicto de intereses y oposición de voluntades del Estado contra otros actores, para imponer una voluntad y/o defender el derecho del uso seguro de este, se puede deducir que, en cautela de los intereses nacionales y de la sobrevivencia del Estado, se establecieron las políticas necesarias o lineamientos para enfrentar la Ciberguerra derivando en el concepto de *Ciberdefensa.*

En cuanto a la *Ciberdefensa*, fue pertinente señalar que, en el contexto nacional, derivado de la Política Nacional de Ciberseguridad, se desprende la Política Nacional de Ciberdefensa, esta fue desarrollada por el Ministerio de Defensa bajo el amparo de la Política de Defensa Nacional. En ese contexto la *Ciberdefensa* fue definida como *"…parte del esfuerzo del Estado por ofrecer seguridad a todos los habitantes, generando las condiciones para poder hacer uso pacífico, equitativo y seguro del Ciberespacio"* (Ministerio de Defensa Nacional, 2017. p:3). De la Política Nacional de Ciberdefensa, se derivó a la elaboración del concepto en el ámbito militar conjunto, donde fue definida como *"la condición caracterizada por un mínimo de riesgos y amenazas en el Ciberespacio, y especialmente al conjunto de políticas, acciones, técnicas y elementos destinados a lograr dicha condición"* (Ministerio de Defensa

Nacional, 2018: p.9). Desde el punto de vista del Ejército, el RDI-20008 “Reglamento de Ciberdefensa” (2016) la define como *"conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno”* (Ejército de Chile, 2016. p:15).

En la búsqueda de elementos comunes dentro de las definiciones en el ámbito nacional se pudo establecer que en todos ellos se identificaron elementos como: normas, técnicas y una intención de obtener una *condición de seguridad,* tanto de los capitales de la información como de las infraestructuras asociadas al ciberespacio, todo lo anterior, “*contribuye a generar en las personas y organizaciones un grado de tranquilidad y confianza tal, que las incentiva a hacer uso del ciberespacio y sus servicios”.* (Kinast, 2019: p.13).

Por otro lado, y en busca de ampliar la comprensión del concepto, encontramos aquella conceptualización que la define como *“capacidad de recursos, actividades, tácticas y procedimientos, para asegurar la capacidad de mando y control de las fuerzas armadas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios para garantizar el libre acceso al ciberespacio”* (Leiva, 2017: p.3). Esta definición, permitió identificar abiertamente la participación de las FAs y la información que estas manejan como medio para garantizar el uso del ciberespacio.

Otra definición que vino a contribuir a la comprensión del concepto es aquella contenida en el texto del Ejército Nacional de Colombia “*Comunicaciones Operacionales y Ciberdefensa 2015”,* que define la Ciberdefensa como;

> …defensa activa y pasiva del centro de operaciones, los medios de información que posee la institución con el fin de repeler los ataques cibernéticos que sufra la institución, al cual su alma rectora por disposición son las comunicaciones militares y coadyuvar a la protección cibernética de la infraestructura crítica del país (Colombia, 2015. p:4).

Por último, el DoD define como *Defensa del Ciberespacio* como;

> …acciones destinadas a proteger el ciberespacio, para vencer a las amenazas específicas que han violado o están intentando infringir las medidas de seguridad del ciberespacio e incluye las acciones de detectar, caracterizar, resistir y mitigar las amenazas incluidos los virus y actividad no autorizada de los usuarios, así como recuperar los sistemas a una configuración segura. Esta es parte de las operaciones defensivas del ciberespacio específicamente las Medidas de Defensa Internas (IDM). (Estados Unidos.2021. p:55).

La ejecución de todo lo anterior, solo es posible con operaciones militares en este *espacio de batalla,* para poder así, enfrentar estas voluntades y determinar la predominancia de una o de otra. Es así, como la Ciberdefensa derivará en acciones militares, surgiendo entonces el concepto de ciberoperaciones.

El Departamento de Defensa de los Estados Unidos (DoD) define las *ciberoperaciones* como *"el empleo de las capacidades del ciberespacio, donde el propósito principal es alcanzar los objetivos en o a través del ciberespacio"* (Estados Unidos, 2019: p.3). Asimismo, esta publicación doctrinaria, estima que estas operaciones *"involucran lo militar, inteligencia nacional y las operaciones regulares del DoD*", además las clasifican en *"operaciones ofensivas en el ciberespacio, operaciones defensivas en el ciberespacio y operaciones de redes de información"*.

De todas las definiciones anteriores y habiendo hecho un recorrido por la discusión planteada en el presente marco teórico-conceptual, fue posible establecer que la *Ciberdefensa* involucra una acción enmarcada en el ámbito militar, en ese sentido, es parte de las decisiones del Estado, ya que tendrá repercusiones en otros estamentos fuera de la seguridad de los sistemas militares. Además, está claramente enmarcada en la protección de un capital físico y abstracto que puede ser amenazado por otro Estado, o bien por actores independientes. Entonces, establecido el espacio de batalla, identificado como ciberespacio, fue factible establecer que en él se desarrollará la ciberguerra o el choque de voluntades para tomar control de este en sí mismo, de los capitales de información e infraestructura crítica que lo componen, o bien será usado para configurar acciones en otros dominios de la guerra.

Esta guerra, como cualquier otra, estará compuesta por una o varias operaciones, que en este caso entendemos como *ciberoperaciones*, las cuáles derivarán de la planificación, concepción y capacidades establecidas en el ámbito de la *Ciberdefensa,* conforme lo plantean las definiciones antes descritas. Habiendo sido el objeto de estudio de la presente investigación, y en ese marco; se identificaron las características que la definen y cómo, a través del análisis de estas, fue pertinente calificarla como un *problema estratégico*.

Habiendo determinado lo anterior, fue importante enmarcar el concepto de *problema estratégico* y, en la amplitud de posibilidades de desarrollar el tema, se declaró que el estudio fue abordado desde el punto de vista de la estrategia, como un nivel de la conducción militar nacional. Durante el trabajo de revisión bibliográfica fue posible determinar que no existe una definición del concepto del *problema estratégico*, no obstante, se pudieron encontrar definiciones específicas al descomponer el constructo, por un lado, el *problema militar* y por otro *estrategia* como nivel de la conducción.

En este contexto, la Doctrina Nacional para la Acción Conjunta define nivel estratégico como;

> planificación y conducción que se ejerce a través de la estrategia militar de carácter conjunta y de responsabilidad del Jefe de Estado Mayor Conjunto. Esta estrategia conjunta es entendida como la ciencia y arte, de concebir y conducir estratégicamente los medios dispuestos por las instituciones armadas, para la preparación y ejecución de los planes estratégicos… para alcanzar el objetivo político de guerra bélico o de crisis (Ministerio de Defensa Nacional, 2011: p.15).

Por su parte el Ejército en su doctrina define la conducción estratégica como;

> *la que realiza el Jefe de Estado Mayor Conjunto (conductor estratégico) sobre todos los órganos de maniobra terrestres, navales, aéreos y conjuntos que se conformen. En la guerra moderna lo normal es la conformación de comandos conjuntos que ejecutan campañas en teatros de operaciones conjuntos.* (Ejército Chile, 2017. p:33).

Lo anterior, aun cuando en los párrafos sucesivos coincide plenamente con la definición de la DNC del 2011.

Otra referencia es aquella usada por Leonhart (1991) en su obra *"El arte de la maniobra"* que definió el nivel estratégico cómo *"nivel de la planificación de la guerra responsable de la aplicación de los medios militares para alcanzar los objetivos nacionales. El nivel de planificación que elabora planes de guerra y objetivos de teatro"* (p.6)*,* finalmente y utilizando una definición de estrategia aceptada por el Ejército, el autor Arthur Lykke[7], la define como *"la articulación de los medios disponibles, de acuerdo con los modos seleccionados, para lograr los fines deseados"* (Berkebile, 2018).

De lo anterior, se pudo inferir que el nivel estratégico está concebido por un conductor militar que debe utilizar los medios disponibles (potencial bélico nacional), buscando los modos particulares para alcanzar los fines u objetivos establecidos por el conductor político, en pos de los objetivos e intereses nacionales. De la ponencia anterior, surgió una incógnita asociada a la determinación de los *modos* para alcanzar los fines, esos modos se adecuarán al problema que se le presenta al conductor estratégico, para transitar de la condición en la que se encuentra hacia el estado final deseado conforme a los fines establecidos. Lo anterior, dio paso a la definición del problema militar y específicamente, conforme a la cantidad de variables que presenta la *Ciberdefensa,* a los tipos de problemas mal estructurados o complejos, o su definición en inglés como *wicked problem*.

El reglamento del Proceso de las Operaciones del Ejército, expone que el problema mal estructurado es aquel en que no existe una formulación clara que parezca factible ya que la información requerida no está disponible, además, implican muchas variables, lo que dificulta su análisis requiriéndose múltiples soluciones, aplicadas concurrente o secuencialmente. De esa manera los que los resuelven, deben separar, a veces, problemas complejos mal estructurados de problemas más pequeños. (Ejército Chile, 2016).

[7] Arthur F. Lykke, Coronel y estudioso militar de los Estados Unidos, autor de "Defining Military Strategy = E + W + M"

Por otro lado, la definición de *"problema perverso",* de su traducción en inglés de *wicked problem,* entiende el problema estratégico como *"un problema más complejo, más que solo complicado, esto debido a que no puede ser removido de su entorno, resolverlo y devolverlo sin afectar otras variables. Además, no existe una relación clara entre causa y efecto"* (Reino Unido, 2017: p.7).

Habiendo hecho la descomposición teórica del tema de estudio *"La Ciberdefensa como problema estratégico",* en cada una de sus partes fue posible iniciar la indagación de las características y aquellas condiciones que contribuyen a poder determinar que efectivamente la *Ciberdefensa* puede ser considerada como un problema para el conductor estratégico, y la consecución de los objetivos e intereses del conductor político.

1.7 Marco Metodológico

1.7.1 Enfoque, nivel de conocimiento y diseño investigativo

Desde el punto de vista del enfoque epistemológico y en coherencia con la naturaleza del tema asociado, se asumió que la *hermenéutica*[8] fue el enfoque más adecuado, considerando que se basó en la experiencia de otros y básicamente la interpretación de documentos (Hernández, 2014), ya que no existiendo aún consenso en muchas de las definiciones de Ciberdefensa o de lo que involucra un problema estratégico, obligó a la comprensión e interpretación de conceptos y significados vinculados al problema de investigación.

Respecto al paradigma de investigación se consideró el de *tipo cualitativo*, ya que se requirió comprender el hecho en cuestión sin realizar modificaciones o intervención de antecedentes (CEEAG, 2017). Por otro lado, derivado de este paradigma, se

[8] La hermenéutica en el ambiente de la investigación se usa como técnica de *interpretación* de textos, conforme lo define Dora Cervantes, *"favorece la discusión al hacer nuevos aportes al desarrollo científico con propuestas que pueden ser cuestionadas permanentemente pero que siempre se orientarán a alcanzar nuevos desarrollos".* (Cervantes, 2017).

ajustó más a las relaciones multicausales asociadas al estudio de las características de la Ciberdefensa y las variables que la determinan como problema estratégico.

Conforme al nivel de conocimiento, fue de tipo descriptivo-interpretativo, existiendo una variada bibliografía en el ámbito nacional e internacional que abordaban tanto la Ciberdefensa, la estrategia y los problemas militares mal estructurados, por lo que se dedujo que, se estaba investigando sobre un tema ya tratado al menos en sus partes, y que obligó al investigador a indagar cuál era el andamiaje preciso que vinculaba ambas partes del objeto de estudio.

Conforme al diseño investigativo, se optó por el *método documental* en atención a que consistía en un proceso sistemático de indagación, análisis e interpretación de datos (Cervantes, 2017), considerando que a partir de este método se podría generar el nuevo conocimiento en la reconstrucción de definiciones, y aproximación al objeto de estudio a partir de un análisis de diferente bibliografía, buscando llegar a un consenso académico aceptable para la realidad institucional.

1.7.2 Universo y muestra

La muestra para la presente investigación estuvo basada en la indagación de bibliografía nacional e internacional, así como individuos, que fueron entrevistados en busca de un juicio de especialistas. Desde el punto de vista de la bibliografía nacional, el enfoque estuvo dado por todos los aspectos relacionados con *Ciberdefensa*, de la Doctrina Nacional Conjunta y aquella pertinente a cada institución de las FAs, por otro lado, se seleccionó como base, además, las actuales publicaciones de estudios en el ámbito de la Defensa y doctrina de Colombia, Estados Unidos, España e Inglaterra, contando con una muestra considerable y que no posee consenso pleno en el objeto de estudio.

Los criterios para la selección de la muestra, primero, desde el punto de vista nacional, se consideró la pertinencia al nivel de la conducción estratégica del Estado Mayor Conjunto y de cada institución, acotando de esta manera a las necesidades del objetivo principal. Por otro lado, la doctrina extranjera, así como las publicaciones e investigaciones afines, fueron seleccionadas en base a que, Estados Unidos,

España y Reino Unido, han sido la doctrina base para la elaboración de la doctrina nacional; segundo desde el punto de vista de los idiomas, fue factible acceder a esta con un mínimo de interpretación por parte del autor, dando la objetividad necesaria a la investigación y por último, la amplia disponibilidad de material de consulta referida al tema de estudio.

Respecto a la selección de Colombia, obedeció primeramente a contar con un referente regional del cono sur, por otro lado, su desarrollo en el ámbito de la Ciberdefensa lo pone a la vanguardia en la región y, por último, su doctrina base también es aquella provista por los Estados Unidos, por lo que se pudieron obtener experiencias basadas en la implementación de esta en la actualidad.

Por otro lado, se optó por consultar a determinados especialistas para la ejecución de entrevistas como técnica de recolección de datos, para esto los criterios de selección de los individuos se basaron en ciertas competencias o características que a continuación se detallan: Oficial de las Fuerzas Armadas especialistas primarios; militares (en servicio activo o condición de retiro) o docentes con grado académico de magister y/o doctorado con experiencia en el ámbito de la estrategia y/o la Ciberdefensa; más de 25 años de experiencia en el rubro de la Defensa; académicos o políticos asociados al objeto de estudio de la Ciberdefensa; autoridades civiles y militares que se desempeñen en el ámbito de la Defensa Nacional y, por último integrantes del Estado Mayor Conjunto asociados a la planificación estratégica y/o Ciberdefensa. Cabe señalar que las características anteriormente descritas son inclusivas entre sí.

Conforme a lo anterior, es pertinente destacar que se tuvo en consideración los criterios de confiabilidad, credibilidad y transferencia para la selección de la muestra, buscando asegurar que, a través de la saturación de conceptos asociados, se aproximara a definiciones aceptables y válidas para la investigación.

1.7.3 Variables y/o factores de análisis

Las factores de análisis seleccionados para la presente investigación fueron:

a) Las *variables operacionales*, que involucran los factores *militares, infraestructura e informaciones.*

b) Los principios de la guerra conjuntos como concepto teórico-práctico y unificador en todos los dominios en donde se desarrolla el conflicto.

1.7.4 Técnicas e instrumentos de recolección de datos

La investigación se basó principalmente en la revisión bibliográfica tanto de doctrina nacional como extranjera, además apoyado en entrevistas, en busca de experiencia y juicio de especialistas, con la intención de obtener percepciones de primera fuente, que aportaran en su ámbito de conocimiento, conforme al desarrollo de cada uno de los objetivos intermedios de la presente investigación.

Respecto a la bibliografía de consulta se ha detallado en el punto 3.2. aquellas que fueron seleccionadas y los fundamentos para ello. Por otro lado, se seleccionaron algunas características o competencias que debían cumplir los individuos que fueron considerados para los fines de este estudio. Para lo anterior, se seleccionó el tipo de entrevista semiestructurada[9], de tal manera de no limitar al entrevistado, pero a su vez, evitar que desvíe el contexto y finalmente se transformara en el instrumento mismo (CEEAG, 2017).

La técnica específica de recolección de los datos fue mediante la técnica de triangulación[10], buscando confrontar tanto la información vertida en la bibliografía como las opiniones de los entrevistados y finalmente el juicio conclusivo del autor.

1.7.5 Método de análisis de los datos

[9] En ellas, el entrevistador prepara un guión con los principales temas a abordar, pero permite que el sujeto exprese sus ideas y opiniones. (CEEAG, 2017: p.108).

[10] Triangulación, se entiende como la convergencia de distintas perspectivas y métodos en el estudio de un mismo objeto, asegurando así una aproximación más comprensiva del problema investigado. (CEEAG, 2017: p.120).

En una *primera etapa,* la recolección y análisis de datos estuvo dada por la exploración de bibliografía nacional y extranjera, de tal manera de generar una base teórica de datos. Estos fueron sometidos a un análisis de contenidos para establecer las relaciones existentes mediante la técnica de triangulación tratada en el punto precedente.

La misma técnica fue usada para la *segunda etapa*, los datos recogidos por las entrevistas de *especialistas*, pudiendo así efectuar un análisis de lo recolectado bibliográficamente y la confrontación de las experiencias para, inferir sobre el objeto de estudio y construir las conclusiones coherentes con el objetivo planteado.

CAPÍTULO II
EL PROBLEMA ESTRATÉGICO

2.1 Metodología del capítulo

El presente capítulo ahondó en el significado del concepto *problema estratégico*, expresión que generó una serie de interrogantes al autor en el sentido de ¿dónde está definido?, ¿cómo está definido?, ¿cómo se genera? y cuyo alcance se delimitó aquí. Para lo anterior, se indagó en diferentes fuentes de información nacionales y extranjeras, así como la opinión vertida por entrevistados relacionados con el área de estudio y la conducción estratégica, con el propósito de construir y proponer un concepto. En concordancia con lo anterior, se logró generar un constructo inicial para la investigación, que aportará finalmente, junto a los capítulos posteriores, a establecer por qué la *Ciberdefensa* se determina como un *problema estratégico*.

Las perspectivas sobre el concepto analizado están acotadas a bibliografía de Chile, Colombia, España, Estados Unidos y Reino Unido. La comparación y análisis a partir de la revisión de estas fuentes abordaron un aspecto netamente teórico y, por otro lado, las opiniones de los entrevistados, el enfoque práctico o experiencial del concepto. Todo lo anterior en el contexto de países referentes para la doctrina nacional, y el estudio del ámbito propio. Lo anterior, permitió identificar que no existe un consenso académico por lo que fue necesario acuñar una definición aplicable a la realidad de la conducción estratégica nacional.

Las fuentes analizadas correspondieron a publicaciones doctrinarias de los países mencionados, así como publicaciones relacionadas con estrategia militar y/o planificación estratégica, además de la información obtenida en las entrevistas, buscando siempre la relación del nivel de la conducción con el problema militar asociado a este, con el propósito de contrastar la teoría con la experiencia.

2.2 Aproximación teórica al origen del concepto

Como fue declarado en el capítulo precedente, no existe una definición tácita del concepto *problema estratégico* en la Doctrina Nacional Conjunta, donde al menos se revisaron los siguientes textos: 1) DNC “Doctrina para la Acción Conjunta de las Fuerzas Armadas”, 2) DNC 3-0 “Doctrina de Operaciones Conjuntas”, 3) DNC 5-0 “Doctrina Conjunta para la Planificación de Operaciones de las Fuerzas Armadas”, y 4) DNC 5-10 “Manual de Planificación Operacional de las Fuerzas Armadas”; en atención a aquello fue necesario explorar otras doctrinas con el fin de comparar y buscar una aplicación a la realidad nacional, no obstante lo anterior, fue factible encontrar definiciones específicas al descomponerlo, abarcando el *problema militar* por un lado y por otro *estrategia o estratégico,* siempre apegado a la delimitación como nivel de la conducción.

En el ámbito de la planificación militar, independiente del nivel de la conducción y de la doctrina desde donde se aborde el tema, se proponen metodologías para afrontar la problemática que ofrece el entorno y una amenaza que se opone a la voluntad propia, a grandes rasgos y sin profundizar en detalles de cada metodología de planificación, se infiere que éstas están orientadas a generar un método de solución de problemas militares, ya que como expresa la doctrina del Ejército de Chile (2016), la solución de problemas es una forma de tomar decisiones.

Conforme a lo expuesto anteriormente y en atención a la necesidad de dar un marco preciso para el desarrollo de los capítulos posteriores, referidos a la *Ciberdefensa*, se procedió al análisis del *problema estratégico,* descomponiéndolo y analizándolo a la luz de diferentes doctrinas y publicaciones, sumado a juicios y comentarios de especialistas, pudiendo acuñar un término concreto para la investigación.

FIGURA 1 Doctrinas estudiadas para analizar las perspectivas

Nota: Figura elaborada por el autor.

2.3 El problema militar

En este punto se realizó la exploración bibliográfica de doctrina y publicaciones de diferentes países, de tal manera de obtener una muestra válida para la generación del concepto.

2.3.1 Chile

El caso de Chile no es distinto a las otras fuentes doctrinarias consultadas, donde no es posible extraer una definición del *problema estratégico* en forma tácita desde su Doctrina Nacional Conjunta, pero sí es posible encontrar diferentes definiciones y explicaciones asociadas al nivel estratégico, conceptos que permiten inferir algunas características de lo que considera el *problema* de este nivel. Para lograr una mayor consistencia de los conceptos, además de revisar la doctrina conjunta, se tomaron algunos antecedentes de la doctrina específica del Ejército, que en dos de sus

publicaciones hace alusión al *problema militar.* Lo anterior, permitió delimitar el marco definido, donde fue posible identificar que en la DNC-0 *"Doctrina para la Acción Conjunta de las Fuerzas Armadas"* del año 2011, no se vierten definiciones del *problema militar,* pero se pudieron deducir aspectos relevantes para la aproximación del concepto. Viene así expresado, que el *ambiente estratégico* es tan complejo que será necesario el empleo de las Fuerzas Armadas (FAs), para un amplio espectro de tareas por cumplir siendo necesario que estas dispongan de capacidades especialmente flexibles, polivalentes e interoperables. Las características de esas capacidades descritas vienen asociadas a la articulación para alcanzar un objetivo estratégico emanado desde el nivel político, en pos de los objetivos nacionales. De lo anterior, solo se pudo rescatar que, en este nivel de la conducción, se deberán articular capacidades para enfrentar *escenarios complejos*.

Por su parte, en la publicación doctrinaria DD-10001 *"La Fuerza Terrestre"* de 2019, acápite de *Ambiente Operacional Futuro*, enmarca la mayor parte de su discurso en la *problemática estratégica* de los diferentes escenarios que se pueden llegar a prospectar conforme a la metodología sugerida. En los pasajes asociados a esto es factible extraer, que es necesario abordar la *complejidad del problema* de este nivel a través de la metodología de análisis de las variables operacionales PEMSII-PT, dejando claro que para este nivel el *problema* o la *problemática estratégica* es multifactorial. Por otro lado, en el apartado de *"Las funciones del comandante en el Proceso de las Operaciones Militares"* establece claramente que en la fase *"Comprensión",* independiente del nivel de la conducción, el comandante debe esforzarse por comprender el *problema militar* que enfrenta. (Ejército de Chile, 2019).

En adición a lo anterior, y de forma mucho más detallada el reglamento del Ejército RDPL-20001*"Proceso de las Operaciones"* edición 2016, destina un punto completo de su primer capítulo al análisis y solución de problemas, de donde se pudieron extraer algunas características propias del *problema militar* asociado al *nivel estratégico.* La primera diferenciación que se identificó es que los problemas no serán todos iguales y que poseen grados de complejidad, y esta estará dada por la cantidad de información con la que se cuenta, por la cantidad de tiempo asociado a su solución y por las variables necesarias a analizar de cada uno de ellos.

De lo anterior se desprenden problemas; 1) Estructurados, 2) Medianamente estructurados, y 3) Mal estructurados. De las categorizaciones anteriores, fue pertinente poner énfasis en aquellos de connotación *mal estructurados*, ya que por sus características de; 1) escasez de información, 2) multiplicidad de variables, 3) estimaciones o predicciones sin respuestas comprobables, obedecen más al concepto de *escenarios complejos* planteado por la DNC y a la metodología de análisis de *variables operacionales*, propuestas por la publicación doctrinaria de *"La Fuerza Terrestre"*. De todo lo anterior, fue factible colegir que la complejidad del problema estará directamente asociado al aumento de variables y a la menor cantidad de información disponible.

De la información obtenida de la doctrina chilena, fue factible reconocer primero que no existen definiciones tácitas de *problema estratégico*; segundo la doctrina conjunta se explaya en el nivel de la conducción estratégica, el cual será tratado posteriormente, pero tampoco hace referencia a problemas en este nivel, más allá de determinar que es un *ambiente complejo*. Por su parte, en la doctrina del Ejército, se pueden extraer mayores antecedentes en general del *problema militar*, y las metodologías sugeridas, lo que permitió entender que los problemas militares en el nivel más alto serán multifactoriales, mal estructurados y sin soluciones estándares establecidas, debido a que se prospectan en escenarios complejos, variables e inciertos.

2.3.2 Colombia

En el estudio e indagación acerca de un concepto o clasificación del *problema militar* no fue posible encontrar algo concreto, pero están presentes algunas características identificables a lo largo de dos de sus publicaciones doctrinarias. Se pudo inferir respecto de los propósitos para los cuáles está formulada la doctrina operativa de Colombia en su nivel conjunto y en el nivel del Ejército como institución. Conforme a lo anterior se señalan a continuación algunas definiciones y consideraciones respecto a los métodos de resolución de *problemas* en el nivel de la conducción estratégica.

En la publicación doctrinaria *"Doctrina"* publicada en el mes de septiembre de 2017, el Ejército Nacional de Colombia hace una distinción clara de los niveles de la conducción militar, específicamente que se entiende y cuáles son las implicancias del *Nivel Estratégico*, las cuales son descritas más adelante en la investigación, pero no fue factible determinar alguna definición específica de *problema militar.* A pesar de lo anterior, se pudo deducir algunos aspectos asociados al tema de estudio, ya que a partir de la definición de los niveles de la conducción, comienzan a diferenciarse los procesos de planificación necesarios para dar cumplimiento a los objetivos impuestos por los respectivos mandos superiores, a partir de los cuáles se pueden identificar las metodologías de solución de *problemas.*

En el texto mencionado anteriormente, se establece que *"… la Doctrina conjunta cubre ampliamente los niveles estratégicos y operacionales…"* (Colombia, 2017. p:23), permitiendo así situar la búsqueda en las publicaciones pertinentes al nivel de la conducción que es de interés para la investigación, y principalmente establecer las características del *problema militar* de este nivel. Específicamente en la caracterización del nivel estratégico, plantea que abordará los *problemas* asociados a los objetivos nacionales, establecidos en la Política y Estrategia de Defensa de Colombia, por tanto, problemas del ámbito nacional, multinacional y del Teatro de Operaciones, que poseen variables múltiples y cambiantes. Se dedujo que, en este nivel y derivado del más alto nivel de planificación nacional, se establecen los objetivos estratégicos, los cuales deberán enfrentar conforme a su dimensión (Teatro, nacional o multinacional) diferentes variables para alcanzar esos objetivos.

Por otro lado, y adentrado en la doctrina terrestre, pero específicamente en lo referido a la aplicación conjunta y a su acápite *"Adaptabilidad Operacional"*, destaca que los líderes en los niveles de la conducción estratégica y operacional deben poseer las características de *adaptabilidad e innovación*, estas características asociadas a los tipos de problemas a los que se verán enfrentados en un ambiente cambiante y de actores múltiples donde las nuevas tecnologías juegan un rol fundamental.

En la publicación doctrinaria *"Doctrina Conjunta",* establece claramente que cada nivel de la conducción posee sus propias problemáticas, dejando de manifiesto que el uso

de la doctrina conjunta va a permitir la estandarización de la terminología y con esto *"…permite a los comandantes de unidades conjuntas y sus estados mayores resolver problemas estratégicos, operacionales y tácticos"* (Colombia, 2018. p:25). Cabe destacar que para la doctrina de Colombia se entenderá que el concepto de *Conjunto* será estructurado para el uso de las *Fuerzas Militares* integradas que incluyen aspectos de; Estrategia Militar Nacional, Planeamiento deliberado y acciones de crisis, Mando y Control de operaciones conjuntas, y Acción unificada del Ministerio de Defensa y asociados interagenciales. Por último, esta misma publicación doctrinaria establece que *"…los líderes políticos y militares deberán considerar el empleo de la fuerza militar en operaciones que se caracterizan por tener la problemática de un ambiente operacional complejo e interconectado, que afectará el empleo de las capacidades militares y depende de las decisiones del comandante…"* (Colombia, 2018. p: 57) y que el uso de la doctrina conjunta y la unificación de su terminología permite estandarizar las relaciones, las responsabilidades y los procesos del Comandante Conjunto y su Estado Mayor *"…con el fin de que estos centren sus esfuerzos en la solución de los complejos problemas que enfrenta en este nivel…"* (Colombia, 2018. p:241).

De todo lo anterior, se pudieron destacar tres aspectos relevantes, primero que en Colombia no solo se identifican los niveles de la conducción, sino que además se asume que cada uno de ellos posee *problemas militares* diferentes, siendo los *problemas estratégicos*, aquellos del más alto nivel militar según esa estructura nacional. Por otro lado, que la doctrina asociada a la planificación estratégica militar está contenida en su Doctrina de Planificación Conjunta, donde se plasman los lineamientos para enfrentar los problemas y así alcanzar los objetivos del nivel político nacional y militar y, por último, se puede rescatar que esta doctrina permitirá dar solución a *problemas complejos.*

2.3.3 España

El caso de España es muy similar a lo que puede presentar el Reino Unido, respecto a los parámetros o marco conceptual establecido por la Organización del Tratado del

Atlántico Norte (OTAN), ya que para su accionar conjunto, combinado y multinacional obedece al mismo marco conceptual de la Alianza. A pesar de ello, fue factible identificar en la doctrina conjunta del Reino de España, algunas características diferenciadoras del *problema* en el *nivel estratégico* de la conducción. Es por ello, que se han obtenido de la Doctrina para el Empleo de las Fuerzas Armadas algunas definiciones que vinieron a contribuir a la investigación.

Un primer alcance al *problema,* lo determina indistintamente del nivel de la conducción, planteando que el *problema militar* o *problema operativo,* es *"aquella situación que enfrenta un comandante cuando debe cumplir una misión dada, con unos medios y en unas condiciones determinadas"* (España, 2018. p:75), seguido de esa definición, aparecen algunos adjetivos al *problema operativo,* donde se declara que, para el cumplimiento de dicha misión, el comandante deberá enfrentar problemas que a menudo serán *complejos y desestructurados.* Por otro lado, la misma publicación doctrinaria plantea que en el *nivel conjunto,* el arte operacional y la elaboración del diseño, permitirán aproximar a estos *problemas operativos complejos, multidisciplinares y desestructurados.*

Por último, se pudo distinguir nuevamente que existe un tratamiento específico para el *problema* en este nivel de la conducción, ya que accediendo al marco regulatorio interno de España, es posible identificar la característica de *multidisciplinario*, y si bien no aparece ni se sugiere alguna metodología o factores de análisis pertinentes para aproximarse a su comprensión, las características de *desestructurado* y *multidisciplinar* permiten inferir que deberán ser tratados por alguna metodología de análisis de los factores operacionales o estratégicos como PEMSII-PT, DIME[11]; como la plasmada en la doctrina de los otros países estudiados.

2.3.4 Estados Unidos

La doctrina conjunta de los Estados Unidos del año 2020, específicamente el *Joint Planning (JP 5-0),* dedica su capítulo IV específicamente para la construcción del

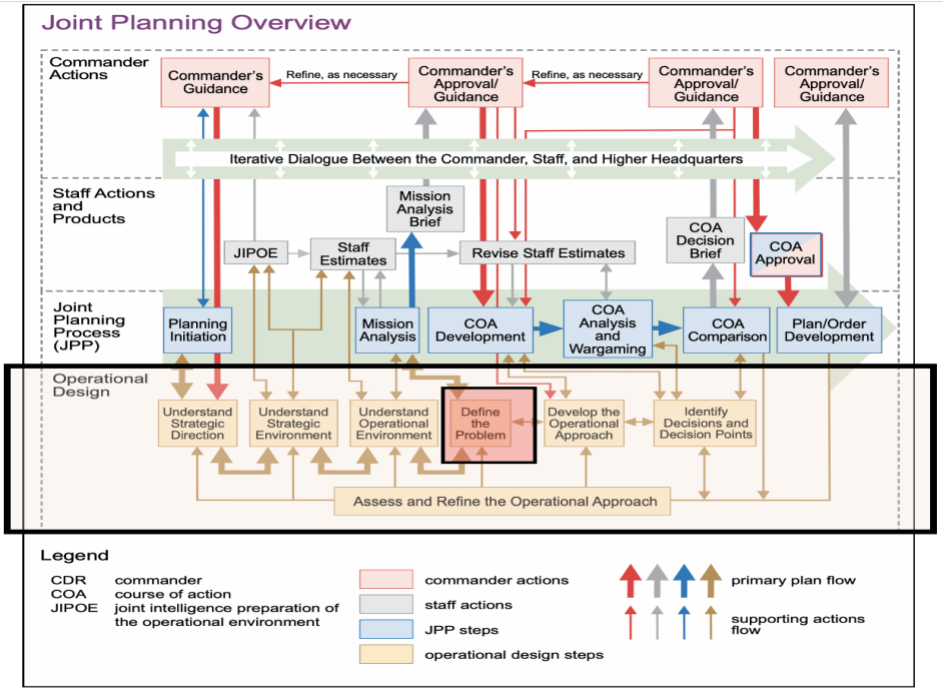
[11] Análisis de los Instrumentos del Poder Nacional *Diplomático, Informaciones. Militar y Económico.*

Diseño Operacional y la comprensión del *problema militar*, y se pudo identificar a lo largo del texto mencionado que en este nivel (conjunto), el problema vendrá definido en 2 documentos de trabajo interno del cuartel general. El primero de ellos es la *Guía Estratégica* y el otro la *Guía del Comandante* (Estados Unidos, 2020). Lo anterior permitió identificar que, si bien no existe una definición explícita, si se posee una conciencia que, a este nivel, el tipo de problemas que se presentan tienen una connotación *estratégica*.

Por otro lado, y enmarcado en la metodología de planificación militar conjunta, se establece que para poder elaborar el diseño operacional es necesario *enmarcar el problema* o bien *"definir el problema, creando una comprensión compartida para una planificación con incertidumbre"* (Estados Unidos, 2020. p: 23). Se pudo apreciar entre líneas que, para este nivel, el *problema militar* requerirá un tratamiento especial, donde primero deberá llegarse a un consenso de lo que se entiende por *el problema,* y luego, se deberán asumir vacíos en esa comprensión que generan el ambiente de incertidumbre. Lo anterior, está gráficamente representado en la *Figura N.º2*, donde se puede identificar el *problema* como aspecto a la par de la comprensión de la *Guía Estratégica, el ambiente estratégico* y la *aproximación operacional.* Además, y haciendo una detención en las conexiones que rodean a la definición del *problema*, este está vinculado con los *flujos prioritarios* para la concepción del plan.

En adición a lo anteriormente expuesto, la doctrina citada expone que para poder desarrollar la estrategia o el plan es fundamental haber definido el *problema*, y surge como interrogante el concepto de la *naturaleza del problema,* haciendo mención que en este nivel es necesario buscar el mayor número de componentes *de facto* para establecer una hipótesis lo más certera posible. Quedó en evidencia que, para este nivel de planificación, el *problema militar* presenta ciertas características que le dan una connotación de *complejidad*, *ambigüedad* e *incertidumbre* donde se expresa que una mala identificación del problema puede generar un problema mayor, afirmación deducida de la expresión *"de hecho, la acción militar lo más probable que exagere el problema en vez de resolverlo"* (Estados Unidos, 2020. p: 36).

FIGURA 2 Identificación del Problema Militar en el Proceso de Planificación Conjunta de los USA.



Nota: Figura obtenida del JP 5-0, Figure III-2 Joint Planning Overview. 2020

Otro aspecto destacado acerca de la definición del *problema militar,* que se identificó en la doctrina, y que a juicio del autor permitió delinear algunas características del *problema estratégico*, es lo que se plantea respecto a la necesidad de observar y examinar los *problemas del nivel conjunto* desde varias perspectivas ya que esto permitirá identificar si el *estado final deseado* de la componente militar está alineado con el objetivo estratégico deseado por el nivel político. La definición precisa del problema en este nivel irá asociado a las capacidades y limitaciones del empleo del potencial militar, pero siempre bajo el amparo de los objetivos nacionales.

Específicamente en el desarrollo del acápite de *Definición del Problema,* se expresan las siguientes características para el problema militar en este nivel: *complejo y mal definido,* incidiendo en la comprensión de este una serie de actores que van

directamente a afectar los factores operacionales y capacidades que se deben considerar para el logro de los objetivos estratégicos.

Por último, y como se expresaba en la aproximación teórica, la doctrina conjunta de los Estados Unidos declara que el *Proceso de Planificación Conjunta* o *JJP* en sus siglas en inglés, está considerado como un medio para la *solución de problemas* que otorga un método a los comandantes y asesores del cuartel general para abordar problemas *complejos* que derivan en el empleo del potencial militar, bajo los parámetros de objetivos estratégicos deseados por el poder político.

2.3.5 Reino Unido

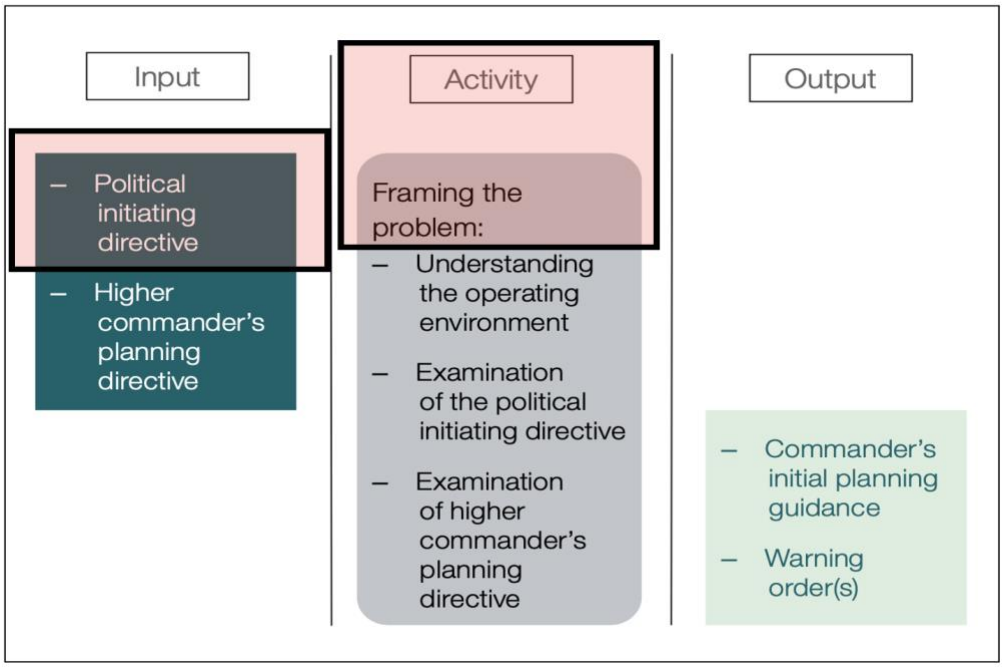
En este caso la doctrina conjunta refiere a la doctrina de planificación conjunta de la Organización de Tratados del Atlántico Norte (OTAN), asumiendo que esta es la base doctrinaria desde donde se abordaron las materias asociadas al nivel de la conducción estratégica, en el que se desarrolló la presente investigación. Es así que, como para el caso de este país, se abordaron las publicaciones tanto de la OTAN como aquellas asociadas a instituciones de estudios como la *Defense Academy of the United Kindom.*

La Doctrina Conjunta Aliada para la Planificación de Operaciones (AJP-5) en su edición 2019, ya en sus primeras páginas al definir el *Arte Operacional* como un proceso y un marco conceptual para planificar y conducir operaciones, establece que *"El arte operacional busca aclarar la situación, evaluar oportunidades y riesgos, fomentar acciones que adquieran ventaja y ofrecer soluciones lógicas a problemas complejos"* (OTAN, 2019. p:1-3). De la definición anterior, proveniente del marco doctrinario de la planificación militar del *nivel estratégico y operacional*, se pudo deducir que el *problema* o los *problemas militares* que le competen son por definición problemas *complejos*. Acto seguido de la definición anterior, establece que el *Arte Operacional* será la manera de poder ir articulando modos, medios, y fines para organizar fuerzas, tiempos y espacio para poder alcanzar los objetivos. De la idea

anterior se pudo identificar claramente el paradigma de Arthur Lykke en su definición de estrategia[12].

En otro contexto, la doctrina aliada asumida por el Reino Unido, se expresan las etapas que deben considerarse en la metodología de planificación en el nivel conjunto, donde a través de un esquema básico de *sistemas,* se hace presente que en la primera etapa denominada *Iniciación* cobra vital importancia la comprensión del *problema* en este nivel, dejando en forma gráfica los *inputs* y *outputs* que lo enmarcan, como sigue:

FIGURA 3 Etapa de Iniciación en el Proceso de Planificación Conjunta de la OTAN



Nota: Figura obtenida por el autor a partir de la imagen obtenida del AJP-5, Table 4.1 Initiation. 2019

Posteriormente a la descripción del esquema, hace mención que, en los niveles de la conducción *estratégico* y operacional, los respectivos comandantes deberán entregar

[12] La definición de Lykke presenta la *estrategia militar* como una fórmula matemática que permite entender fácilmente las variables de la *estrategia.* la variable dependiente en el lado derecho de una ecuación es el resultado o estado final deseado. En la práctica, la variable dependiente es un estado final y la ecuación del proceso estratégico debería abarcar cuatro variables, estas son: *fines* (objetivos), *modos* (conceptos), *medios* (recursos) y estado final (estado final militar). (Berkebile, 2018).

las guías de planificación considerando al menos; 1) la compresión del ambiente operacional, 2) *el problema,* y 3) la misión establecida por el nivel político.

De la *Figura N.º3*, se puede desprender que en este nivel se reciben las *entradas* desde el nivel político y las directrices del comandante del más alto nivel (estratégico), dejando claro que el problema militar posee influencia relacionada con estado final deseado político y considera variables muy amplias, pudiendo inferir que demanda un análisis sistémico más allá de lo militar.

Por otro lado, esta misma publicación establece que es la *orientación estratégica* la que aborda *problemas complejos* y que al estar inicialmente incompleta, podría necesitarse además una interpretación antes de ser transmitida a los niveles inferiores, asumiendo que serán los niveles político-militar y *el comandante estratégico*, quienes poseen claridad en la perspectiva estratégica que se les presenta. En este párrafo quedaron de manifiesto dos elementos claves para la investigación, primero la característica *complejo* que se le asigna al problema de este nivel y segundo que se asume que es un problema del nivel político-militar y del *comandante estratégico.*

Conforme a lo expresado en este texto doctrinario, se pudo identificar una serie de elementos respecto al problema militar en este nivel de la conducción, quedando establecido primeramente que es un *problema complejo*, por otro lado, *incompleto* atendiendo a que desde que se genera la necesidad las variables no están todas abordadas y que en ese contexto la responsabilidad de interpretarlas y traducirla a los niveles más bajos recae en el *conductor estratégico.*

Otra publicación que fue pertinente para el análisis respecto a la doctrina del Reino Unido, asociada a la OTAN es la publicación doctrinaria AJP-3 *Allied Joint Doctrine for the Conduct of Operations.* En esta se establecen parámetros similares a la doctrina expuesta anteriormente, no obstante se pudieron identificar algunas caracterizaciones de los problemas que complementan la investigación, en su Sección N.º2 *"Principios y consideraciones operacionales de las operaciones conjuntas y multinacionales",* establece que la aplicación del método orientado por estos principios y consideraciones permitirá hacer una aproximación más concreta acerca de los

problemas de este nivel, que se caracterizan por ser *complejos y dinámicos.* (Reino Unido, 2019)

Por otro lado, esta misma publicación establece en la descripción de los *principios del mando conjunto,* que la mejor manera de poder entender la naturaleza del *problema* es: 1) entender el contexto estratégico, 2) el uso de herramientas de comprensión e integración del ambiente operacional, 3) evaluación de actores. Todo lo anterior para permitir al *comandante estratégico* una comprensión de factores intangibles y mucho más amplios que afectan el *problema.*

A través del análisis de esta publicación fue posible identificar nuevamente que resaltan características del *problema militar* de este nivel, esta vez lo determina como *complejos y dinámicos*, y por otro lado al analizar los parámetros sugeridos bajo el concepto de principios de la planificación y conducción conjunta, se expresa tácitamente que la metodología debe iniciar con la comprensión de la *naturaleza del problema*, a través de variables amplias y que aborden influencias tangibles e intangibles del ambiente. (Reino Unido, 2019)

Otra publicación que fue atingente para el análisis conforme al nivel planteado es aquella que emana la *Defense Academy of the United Kingdom*, en su publicación *Getting Strategy Right (enough)*, en la cual hace una descripción de varios aspectos que fueron atingentes al tema de estudio, donde ya en las primeras páginas caracteriza el *problema* del nivel estratégico como *adaptativo o wicked* problema. El término *adaptativo* lo define Ronald Heifetz, para definir aquellos *problemas* que no pueden ser resueltos de maneras convencionales y donde *"se requiere innovación y una observación permanente del problema"* (RCDS, 2017). Por otro lado, el término *wicked,* ha sido descrito anteriormente, pero entendido básicamente como *problema* con una solución *compleja*, donde la incidencia de muchos factores hace que sea difícil o imposible de ser abordado por variables separadas, sin afectar el entorno de igual manera, incluso no es factible determinar la correlación causa efecto claramente.

Así mismo en el texto citado, especialmente en el acápite de *Aplicación de la Estrategia*, donde establece que: *"...la necesidad de una agilidad y flexibilidad*

integradas para adaptarse cuando las situaciones cambian, como sin duda ocurrirá, en parte porque nunca es posible conocer al 100% el problema que hay que abordar" (RCDS, 2017. p:8) y por otra parte expresa *"…Incluso cuando los objetivos políticos están claros, los problemas a nivel de gran estrategia suelen ser tan complejos que es probable que las áreas de incertidumbre persistan hasta bien entrada la implementación de la estrategia"* (RCDS, 2017. P:8). De ambas citas anteriores fue posible determinar que, primero el *problema* en este nivel mantendrá una *mutación*[13] permanente, y segundo el grado de *incertidumbre* respecto a lo que se enfrenta.

Por otra parte, en el título "*Una Guía para la Evaluación Estratégica",* se establece y sugiere una de las metodologías de análisis y comprensión del ambiente estratégico donde se propone el marco conceptual de *STEEPLEMS*, de sus siglas en inglés *social; tecnológico, económico, ambiente, político, legal, ético, militar y seguridad*, asegurando que bajo este análisis al menos las posibilidades de dejar aspectos de relevancia fuera, son menores. (RCDS, 2017.)

Por último, es preciso señalar que ha sido factible identificar en esta publicación, algunos conceptos un tanto distintos a los anteriores donde se agregan las características de *adaptativos* y *wicked*, entendiéndolo como un *problema complejo*. Complementando lo anterior, se manifestó un nuevo marco para el análisis del ambiente estratégico, pero al detenerse a hacer coincidir las variables de análisis propias los puntos en común al menos son: 1) Político, 2) Social, 3) Económico, 4) Militar. Lo anterior permitió nuevamente afirmar que el *problema* del nivel estratégico posee características distinguibles de otros.

2.4 El Nivel de la Conducción Estratégica

A diferencia de la problemática encontrada en la búsqueda del concepto de *problema militar* del punto anterior, el *nivel estratégico* de la conducción es desarrollado ampliamente por cada una de las doctrinas analizadas, existiendo diferencias entre

[13] El concepto de *mutación* viene a hacer referencia a que el problema irá cambiando tan rápido como cambia el ambiente, es un factor que no se puede controlar.

ellas, conforme a las estructuras nacionales, integración de alianzas y por supuesto conforme a los intereses y objetivos nacionales de cada uno de ellos.

2.4.1 Chile

Para el caso de Chile, y como fue expuesto en el marco teórico, la Doctrina Nacional para la Acción Conjunta define nivel estratégico como:

> Planificación y conducción que se ejerce a través de la estrategia militar de carácter conjunta y de responsabilidad del Jefe de Estado Mayor Conjunto. Esta estrategia conjunta es entendida como la ciencia y arte, de concebir y conducir estratégicamente los medios dispuestos por las instituciones armadas, para la preparación y ejecución de los planes estratégicos… para alcanzar el objetivo político de guerra bélico o de crisis. (Ministerio de Defensa Nacional, 2011: p.15)

Esta definición está plenamente compartida por el Ejército de Chile en su doctrina, aun cuando amplía el concepto, expresando que la conducción estratégica es:

> …la que realiza el Jefe de Estado Mayor Conjunto (conductor estratégico) sobre todos los órganos de maniobra terrestres, navales, aéreos y conjuntos que se conformen. En la guerra moderna lo normal es la conformación de comandos conjuntos que ejecutan campañas en teatros de operaciones conjuntos. (Ejército Ch., 2017. p:33).

Cabe hacer presente que, en la doctrina nacional, se hace una diferenciación ampliada de la definición anterior del *nivel estratégico*, vertida en el primer capítulo de la DNC, ya que el capítulo segundo está dedicado al *Nivel Estratégico Conjunto,* donde se expresa que:

> …en este nivel se ejecuta el mando de todas las fuerzas (terrestres, navales, aéreas y conjuntos) asignadas a las operaciones, en una aplicación integrada y sincronizada de todas sus capacidades disponibles, dirigidas por un solo mando,

a través del amplio panorama de las operaciones militares. (Ministerio de Defensa Nacional, 2011. p:22)

Luego expresa nuevamente que el mando estratégico recaerá sobre el Jefe del Estado Mayor Conjunto (JEMCO) y que la planificación que realiza con el Estado Mayor Conjunto será el medio para alcanzar los objetivos políticos y estratégicos a través de *opciones de respuesta militar* (ORM). Todo lo anterior finaliza con la *Directiva Estratégica* que dará el marco de planificación al nivel operacional y táctico.

De los párrafos anteriores se pudieron identificar y extraer ideas claras acerca de los alcances del *nivel estratégico* para Chile, primero que es el nivel militar que traduce los objetivos políticos y políticos de guerra bélico a las fuerzas militares; segundo que el mando estratégico es ejercido por la figura de una sola persona representada por el JEMCO, tercero que la manera de alcanzar los objetivos exigidos por el nivel político darán inicio a la planificación estratégica obteniéndose *opciones de respuesta militar*; y cuarto que la Directiva Estratégica será el documento que da inicio a las planificaciones subsidiarias para los niveles inferiores.

2.4.2 Colombia

Las consideraciones que ha adoptado Colombia como nación respecto al *nivel estratégico* de la conducción tienen semejanzas con la doctrina de Chile, no obstante, fue factible identificar algunas diferencias. En su publicación *Doctrina Conjunta*, establece primero que es un *nivel de la guerra* que comparte clasificación con los niveles operacionales y tácticos. Por otro lado, hace una breve descripción de lo que se entiende por estrategia para poder definir este nivel, donde expresa que *"… es un conjunto de ideas para emplear los instrumentos del poder nacional de manera sincronizada e integrada, con el fin de lograr objetivos del teatro y multinacionales"* (Colombia, 2018. p:40). Es en ese marco, en que Colombia define finalmente que el *nivel estratégico* es aquel;

> …en el cual una nación, a veces como miembro de un grupo de naciones, determina los objetivos y la orientación de seguridad estratégica nacional o multinacional (en una alianza o coalición), luego desarrolla y utiliza los recursos nacionales para alcanzar esos objetivos. (Colombia, 2018. p:40).

Por otro lado, en Colombia se reconoce como conductor estratégico al Presidente de la República, asesorado por el Consejo de Seguridad Nacional, a través del cuál se definirán los objetivos políticos y estratégicos nacionales, aun cuando en párrafos posteriores establece que este nivel será considerado como la *Gran Estrategia*. En adición a los conceptos y estructura anterior se expresa que será el Ministro de Defensa Nacional quien *traducirá* los objetivos estratégicos de la nación en *objetivos militares estratégicos.* El análisis anterior, permitió identificar el estado final militar e iniciar la *planificación estratégica* del teatro para ser ejecutada por los comandantes de los Comandos Conjuntos. Se hace ver que el conductor estratégico sobre los comandos conjuntos será el *Comandante del Teatro de Guerra de la Fuerza Militar.* (Colombia, 2018) La misma publicación determina además que en *nivel estratégico será del ámbito de competencia de 1) Política Nacional y 2) Estrategia del Teatro.*

FIGURA 4 Cuadro comparativo de los niveles de la conducción militar entre Chile y Colombia

Asimilación de los Niveles de la Conducción	
	
Político	Gran Estrategia
Estratégico	Estratégico
Operacional	Operacional
Táctico	Táctico

Nota: Figura elaborada por el autor.

Tras la exploración de la publicación doctrinaria de Colombia, se consiguieron extraer los siguientes puntos concretos, primero que existe un conductor de la *Gran Estrategia* que es el Presidente de la República, que asesorado por el Consejo de Seguridad Nacional, planifican la Estrategia Nacional de Defensa; segundo que la figura del Ministro de Defensa Nacional es quien articula y traduce los objetivos políticos en objetivos estratégicos militares; tercero que el Conductor Estratégico será el Comandante de Teatro de Guerra de las Fuerzas Militares; y cuarto, que el *nivel estratégico* está considerado como un nivel de la guerra ya sea nacional o multinacional.

2.4.3 España

En el caso de España se han revisado las publicaciones del empleo terrestre de las fuerzas y aquellas de nivel conjunto, pero al detectarse la clara correlación que existe en la jerarquía de la doctrina, solo fue pertinente analizar el *Glosario de Terminología Conjunta* y la *Doctrina para el Empleo de las FAs.*

Conforme al marco seleccionado, la publicación correspondiente al glosario militar establece primero que existe específicamente un *nivel estratégico militar* y asociado a esta clasificación, la definición correspondiente los describe como;

> el nivel superior de planeamiento y conducción de las actividades operativas de las FAS, tanto para las operaciones militares, como para la contribución militar a actividades de otros instrumentos de poder, ya sea en el ámbito nacional o en el multinacional. En este nivel se concibe y aplica la estrategia militar y se asesora al presidente y al ministro de Defensa en la dirección estratégica de las operaciones. (España, 2020 p:40).

Por otro lado, la misma publicación establece que los objetivos estratégicos serán aquellos que van a contribuir a la consecución de la condición final deseada a nivel nacional, y estos objetivos derivarán del proceso de *planeamiento estratégico*, el cual establecerá los modos para alcanzar los fines del nivel político-estratégico.

FIGURA 5 Cuadro comparativo de los niveles de la conducción militar entre Chile y España

Asimilación de los Niveles de la Conducción	
	
Político	Gran Estrategia
Estratégico	Estratégico
Operacional	Operacional
Táctico	Táctico

Nota: Figura elaborada por el autor.

En adición a lo anterior y abiertamente con un nivel de desarrollo conceptual más amplio la publicación doctrinaria española del empleo conjunto dedica su capítulo 5to al *Nivel Estratégico Militar.* Es aquí, donde primero la definición del *nivel estratégico* es concordante a la del párrafo precedente. Por otro lado, se declara que los efectos de la estrategia militar van a contribuir a su *Estrategia de Seguridad Nacional.* Del mismo modo, expresa que el *Jefe del Estado Mayor de la Defensa (JEMAD),* será la autoridad estratégica militar, y establece que *"… la autoridad del nivel estratégico puede conducir y planear varias operaciones diferentes que se desarrollen simultáneamente en distintas locaciones"* (España, 2019. p:108). Lo anterior expresa en forma tácita que será un mando único. Además, añade que para la planificación y conducción contará con el *Estado Mayor Conjunto de la Defensa.* Por último, y en atención a la integración de España en la OTAN, todas las descripciones anteriores son aplicables a la doctrina nacional, ya que para la Alianza el *nivel estratégico* corresponde al SACEUR[14], y para el Caso de la Unión Europea (UE) es el director del EUMS[15].

Respecto a la planificación del *nivel estratégico*, establece que el planeamiento iniciará con el análisis de la naturaleza del *problema* y principalmente identificando los objetivos que materializan las condiciones demandadas por el nivel político,

[14] SACERUR, de sus siglas en inglés "*Comandante Supremo Aliado en Europa".* Traducción Realizada por el Autor.
[15] EUMS, de sus siglas en inglés "*Cuartel General Militar de la Unión Europea". Ídem*.

proponiendo a este las diferentes *opciones de respuesta militar* (MRO), las cuales finalmente serán desarrolladas y emanadas en la *Directiva Estratégica.*

De todo lo anteriormente discutido, fue factible identificar en la doctrina de España que: primero; existe un nivel militar de conducción de connotación superior a todas las fuerzas, segundo; ese nivel está dirigido por un mando único, materializado por el JEMAD, tercero; los objetivos estratégicos emanados por el nivel político derivarán en *opciones de respuesta militar* (MRO), que se condicen con el uso del poder militar en beneficio del cumplimiento de los intereses nacionales, cuarto; en el proceso de planeamiento se analizará la naturaleza del *problema* en este nivel, para luego, junto con la ORM seleccionada, generar la *Directiva Estratégica* para dar inicio al ciclo de planificación militar y ejecución de operaciones en los distintos niveles.

2.4.4 Estados Unidos

Antes de ir en busca de la aproximación del concepto de *Nivel Estratégico de la Conducción* en la doctrina de los Estados Unidos, fue preciso señalar y comprender que, debido a su estructura, principalmente a sus objetivos nacionales y estratégicos, a su Política de Defensa Nacional y a su Estrategia de Defensa, los niveles de la conducción de esta doctrina no son similares a los de la doctrina de Chile, esta aclaración fue pertinente para la definición posterior del *nivel estratégico de la conducción*, siendo más preciso explorar en la doctrina de planificación conjunta de los Estados Unidos, asociada a cómo trabajan sus *Comandos Combatientes*[16] para la homologación al nivel del conductor estratégico nacional.

Conforme a los objetivos globales que posee Estados Unidos, como país y como estructura militar, posee particularidades especiales respecto a la aplicación de los *niveles de la conducción*. Debido a lo anterior, además de la doctrina conjunta, se han analizado algunas publicaciones referentes a *Estrategia,* con el único fin de eliminar algún sesgo predeterminado y buscar puntos en común o abiertamente generar la

[16] Comandos Combatientes, *"Mando unificado con una amplia misión continua, bajo un único comandante designado por el Presidente, a través del Secretario de Defensa y con el asesoramiento y la asistencia del Jefe del Estado Mayor Conjunto. También llamado CCMD.* (Estados Unidos, 2021.p: 38)

diferenciación con las otras doctrinas. Actualmente la doctrina de los Estados Unidos JP 3-0, así como el diccionario del Departamento de Defensa *"Dictionary of Military and Associate"* 2021, establecen que:

> La estrategia desarrolla una idea o conjunto de ideas sobre las formas de emplear los instrumentos del poder nacional de forma sincronizada e integrada para lograr los objetivos nacionales, multinacionales y de teatro. El Secretario de Defensa, traduce estos objetivos en objetivos militares estratégicos que facilitan la planificación estratégica del teatro[17]. (Estados Unidos, 2021. p:203).

FIGURA 6 Cuadro comparativo de los niveles de la conducción militar entre Chile y Estados Unidos

Asimilación de los Niveles de la Conducción	
	
Político	Estratégico
Estratégico	
Operacional	Operacional
Táctico	Táctico

Nota: Figura elaborada por el autor.

Por otro lado, y como fue expresado en el Marco Teórico, existen algunas definiciones del *nivel estratégico* de la conducción que son ajenas a la doctrina, pero igual de pertinentes como la del Lt.Col. Robert Leonhart (1991: p.6) en su obra *"El arte de la maniobra",* define el *nivel estratégico* cómo *"nivel de la planificación de la guerra responsable de la aplicación de los medios militares para alcanzar los objetivos nacionales. El nivel que elabora planes de guerra y objetivos de teatro".*

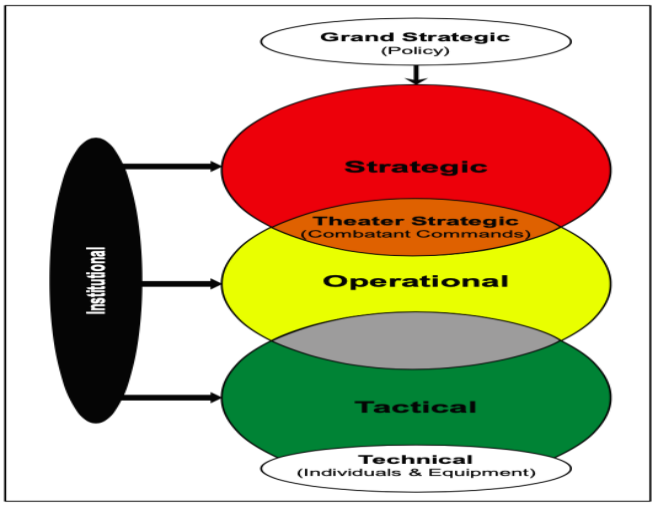
En otra definición y explicación es factible identificar que existe una diferencia entre *estrategia* y *estrategia militar,* donde el Departamento de Defensa de los Estados Unidos (DoD), establece que la *estrategia militar* estará al servicio de la *Política*

[17] Traducción realizada por el autor.

nacional dejándolo como definición *"… un amplio curso de acción o declaraciones de orientación adoptadas por el gobierno a nivel nacional en busca de objetivos nacionales"* (Finney N., 2020. p:6), todo lo anterior, permite complementar la doctrina nacional con otros pensadores, queda reducido el concepto al diálogo dictado por los políticos que deben ser traducidos por profesionales de las armas, quienes serán el puente para alcanzar los objetivos nacionales.

En el caso de la *Estrategia Nacional Militar*, será generada por el Estado Mayor Conjunto *(Joint Staff)*, la cual deberá describir los objetivos militares extraídos de la *Estrategia de Seguridad Nacional*. Todo esto que está generado a nivel de la nación deberá ser entregado a los comandantes de los *Comandos Combatientes* que, si bien por la estructura representan al mando operacional, su envergadura demanda la generación de sus propias *estrategias*, las que no deben ser confundidas con el *nivel estratégico* en estudio. Para una mejor comprensión, lo anterior se expresa a continuación en la *Figura N.º7*.

FIGURA 7 Los Niveles de la Guerra, incluido el nivel institucional



Nota: Figura obtenida de: *Figure 8.1. "The levels of war". Army University Press. 2020.*

La *Doctrina Conjunta* de los Estados Unidos por su parte define el *nivel estratégico como "… el nivel de guerra en el que una nación, a menudo como miembro de un grupo de naciones, determina los objetivos y la orientación de la seguridad estratégica nacional o multinacional (alianza o coalición), y luego desarrolla y utiliza los recursos*

nacionales para lograr esos objetivos" (Finney N., 2020. p:4), así mismo esta doctrina establece que para la guerra existirán los tres niveles 1) Estratégico; 2) Operacional; y 3) Táctico.

En la publicación doctrinaria JDN 2-19 *"Strategy"* (2020), se establece claramente que será el *Departamento de Defensa* (DoD) quién proveerá las opciones de respuesta militar al nivel político, para asegurar a su presidente negociar desde una posición de fuerza. El rol del DoD como *nivel estratégico* militar, está claramente delimitado por los roles que juegan los otros instrumentos del poder nacional, pudiendo según sea la situación colocarse en una posición de apoyo o bien ser el protagonista cuando el empleo del potencial militar es directo. (Estados Unidos, 2020).

Conforme a la discusión generada tanto en doctrina conjunta como en publicaciones afines de estrategia y el nivel estratégico ha sido factible precisar lo siguiente: primero, Estados Unidos distingue entre nivel estratégico nacional y *nivel estratégico militar;* segundo, el *nivel estratégico militar* está al más alto nivel nacional y enmarcado en el DoD, por lo que cumple un rol directo como elemento del poder nacional, como protagonista o como apoyo a otro actor según sea la necesidad; tercero, pudo identificarse que en este nivel existe la figura del *Joint Staff*, o Estado Mayor Conjunto, quienes serán los responsables de generar las opciones de respuesta militar y articular los objetivos del nivel político con aquellos objetivos esperados de sus *Comandos Combatientes*, quienes a su vez generarán su propia estrategia, lo que no quiere decir, que siguen siendo parte del nivel operacional. Conforme a lo anterior el *nivel estratégico* está íntimamente ligado al nivel político sin existir una figura política estratégica o una diferenciación como fue expresado en la *Figura N.º6.*

2.4.5 Reino Unido

Al igual que en la definición del *problema militar*, los textos empleados para el caso del Reino Unido fueron tanto Doctrina Conjunta como publicaciones doctrinarias asociadas a la estrategia. Es así como en la publicación del *Royal College of Defence Studies* (RCDS) del año 2017 *"Getting Strategy Right (enough)"* establece que existe una jerarquía claramente definida en la doctrina de defensa del Reino Unido, esta jerarquía reconoce cuatro niveles de conducción, 1) Gran Estrategia; 2) Estrategia

Militar; 3) Operacional; y 4) Táctico. Para una mejor comprensión de esta jerarquía ha sido pertinente recalcar que la *Gran Estrategia* comprende el mando total del gobierno de la Reina y donde se articulan los elementos del poder nacional: Diplomático; Informaciones; Militar; y Económico (DIME). Para el caso de la *estrategia militar*, solo corresponde al ámbito militar de los factores DIME y esta responsabilidad recaerá sobre el Ministro de Defensa, además será reconocido como el nivel más alto en el ámbito militar, donde el desarrollo de capacidades, acción y sostenimiento de las fuerzas deberán ir en directo apoyo a la política nacional, para alcanzar sus objetivos, los cuáles han sido establecidos por la *Gran Estrategia.* (RCDS, 2017)

Por su parte, la doctrina conjunta, específicamente en la JWP 5-00 *"Joint Operations Planning"* (2018), su primer capítulo está dedicado al *nivel estratégico* y las consideraciones de planificación. En este capítulo, abiertamente en concordancia con la jerarquía de niveles expresadas en el párrafo anterior define que *"…en el nivel estratégico, la estrategia política está diseñada para establecer o dirigir un conjunto de objetivos nacionales o multinacionales en apoyo de los objetivos políticos…"* (Reino Unido, 2018. p:10). Claramente se puede identificar que en este nivel se articularán las fuerzas militares en pos de los objetivos planteados por el político, específicamente en el ámbito militar, como parte de los otros elementos del poder nacional. Además, explica que, en la *Doctrina de Defensa Británica*, este nivel en términos sencillos deberá organizar fines, modos y medios, y que *"… las articulaciones la esencia de la planificación en el nivel estratégico" (*Reino Unido, 2018.*)*

FIGURA 8 Cuadro comparativo de los niveles de la conducción militar entre Chile y Reino Unido

Asimilación de los Niveles de la Conducción	
	
Político	Gran Estrategia
Estratégico	Estratégico
Operacional	Operacional
Táctico	Táctico

Nota: Figura elaborada por el autor.

Por último, al igual que el caso de España, el nivel estratégico británico tendrá ciertas consideraciones al momento de articularse como parte de las fuerzas de la OTAN o bien de la UE, es así como aplicarán los mismos comandantes designados de este nivel dependiendo de la estructura organizada, sabiendo que si es de la Alianza será el SACEUR y si la estructura está bajo el mandato de la Unión Europea será el EUMS.

De las definiciones analizadas y de las particularidades del Reino Unido fue factible identificar que: primero, existe una jerarquía que encuadra el *nivel estratégico militar* bajo la *gran estrategia* que dependerá del nivel nacional (DIME); segundo, que conforme a los intereses nacionales del Reino Unido, el *nivel estratégico* será el responsable de organizar los medios, modos y fines, siendo esta *articulación* el principal oficio del *nivel estratégico militar*; tercero, y último, el mando de este nivel recaerá sobre el Ministro de Defensa del Reino Unido en el caso que se establezca en forma independiente, pero en caso de encontrarse articulado bajo el mandato de la OTAN o de la UE, la responsabilidad del *nivel estratégico militar* recaerá sobre los mandos designados y la planificación asociada será para alcanzar los objetivos políticos de la Alianza o la Coalición determinada.

2.5 Resultados del capítulo

En el presente acápite se exponen los resultados obtenidos luego de la comparación e integración de los conceptos para finalmente establecer el marco que rigió la presente investigación en torno al *problema estratégico.* En primer término, se exponen los conceptos claves extraídos de cada doctrina para luego articular el concepto deseado de manera objetiva y con el rigor científico esperado.

2.5.1 Concepto Problema Estratégico

A partir del análisis de contenido realizado en este capítulo, ha sido posible identificar elementos esenciales en cada perspectiva, que permiten comprender las expresiones de *problema militar* y *nivel estratégico,* para construir el concepto de *Problema Estratégico*:

Nivel estratégico

- Articula los medios y modos para alcanzar los fines políticos.
- Más alto nivel militar.
- Se articula con otros elementos de poder del Estado.
- Se aglutina bajo un mando único.
- Concentra la totalidad de las Fuerzas Armadas o militares de la nación.
- Posee metodología de solución de problemas y planificación.
- Sus productos conforman la Directiva para los niveles operacional y táctico.
- Puede articularse para conflictos nacionales o multinacionales.
- Utiliza perspectivas a largo plazo y supuestos del entorno estratégico del Estado.

Problemas militares en el alto nivel

- Mal estructurados o desestructurados.
- Incompletos.
- Mal definidos.
- Complejos.
- Escasez de información o inciertos.
- Variables interconectadas.
- Cambiantes o dinámicos.
- Multidisciplinares.
- Ambiguos.
- Adaptativos.
- Es necesaria una metodología amplia u holística para entender su naturaleza.

Definición de Problema Estratégico

Una vez establecidas las bases del concepto fue necesario procurar una definición más precisa del término *problema estratégico*. La definición que se ha propuesto no ha pretendido establecer una máxima y dar por completada la discusión académica, más bien la intención fue exclusivamente entregar un marco objetivo para dar tratamiento a las características de la Ciberdefensa y sus particularidades para la conducción militar, siendo este marco el punto de inicio de la investigación.

En consecuencia y consideración, ante las diferentes perspectivas enunciadas, es posible definir el *Problema Estratégico* como:

Dilema del ámbito militar del más alto nivel, que se interpone entre la situación actual y los objetivos esperados por el Estado que, por las características de complejidad, incertidumbre, dinamismo e interdependencia, demandan de una metodología de análisis de variables múltiples para aproximarse a su naturaleza, permitiendo así establecer una opción de respuesta, empleando el poder militar de la Nación[18].

Por lo tanto, es posible concebir este concepto como una relación de interdependencia entre las materias que debe tratar el *conductor estratégico* junto con su equipo de planificación y los problemas del entorno de dicho nivel del Estado, que requieren el empleo de las capacidades militares para el acometido de sus objetivos políticos.

2.6 Validación de los resultados

Para garantizar la calidad de los resultados del presente capítulo, durante la investigación se realizaron entrevistas a especialistas para validar el análisis y comprobar que se ha aproximado de manera correcta a la expresión de *problema estratégico*.

Los entrevistados en esta etapa del proceso fueron los Generales de División John Griffiths Spielman; Rodrigo Pino Riquelme y Pedro Varela Sabando; el General de Brigada Mario Grez Casanueva; los Coroneles Álvaro Vera Soto y Harold Burbano Goyes (COL); el Capitán de Fragata Roberto Siña Lazo y el Teniente Coronel Jorge Villarroel Rivera; por último, el señor don Gonzalo Díaz de Valdés Olavarrieta, que, al ser consultados por el concepto de *problema estratégico*, su definición y alcances, manifestaron lo siguiente:

[18] Definición elaborada por el autor.

Tabla 1 Opiniones de expertos referidos al problema estratégico

Objeto de la pregunta	Especialista	Información obtenida
Características del problema militar en el nivel estratégico	GDD. GRIFFITHS	"no estoy de acuerdo con que se plantee que el problema está mal estructurado, la estructura del problema es la responsabilidad del Oficial de Estado Mayor, estoy de acuerdo que a mayor el nivel de la conducción son el mayor número de variables, es más complejo sin duda. Esta complejidad está dada por la capacidad de consecución del objetivo, con un nivel de incertidumbre alto" (2:00)
	GDD. PINO	¿Cómo dar respuesta al requerimiento desde el escalón político? Ese es el gran problema, la articulación de los medios y los modos. (respecto a la Defensa nacional) (2:00). El nivel de complejidad o estructuración dependerá de lo que necesita el poder político, y en este nivel es multifactorial (3:25)
	GDD. VARELA	El gran problema de este nivel es que sobrepasan el accionar militar, lo que requiere un profundo análisis del ambiente estratégico, considerando que la opción de respuesta militar que va a ser contribuyente a otros elementos del poder nacional. (1:35) Es un problema mal estructurado, por la gran cantidad de variables que lo afectan, y por más que se analice todo, no se asegura el éxito de solución, se pude acortar la brecha sin duda, pero eso es lo complejo. (2:34). Un ejemplo claro es la salida abrupta de USA de Afganistán.
	GDB. GREZ	Siempre enmarcado en el tema de la Ciberdefensa, el problema estratégico está afectado por múltiples variables, donde los límites entre un nivel y otro son difusos, esa condición de incertidumbre lo hace complejo y si además sumamos que no es estático más complejo aún.
	CRL. VERA	Desde mi punto de vista, es complejo y está afectado por muchas variables, pero principalmente lo veo por el desarrollo de capacidades para poder dar satisfacción al nivel de esfuerzo exigido a la fuerza en el contexto de los objetivos políticos de la Nación.
	CF. SIÑA	Es complejo, tiene demasiadas variables, aspectos legales que limitan más que permiten, normalmente la planificación estratégica para alcanzar los objetivos va asociada a desarrollo de capacidades para poder cubrir brechas y cumplir objetivos realistas, se debe buscar un equilibrio entre el objetivo y lo que soy capaz de hacer. Además de tener que articular el idioma entre las mismas instituciones.
	TCL. VILLARROREL	El problema se vuelve mucho más complejo y mal estructurado que en los niveles inferiores de la conducción militar. Este conductor militar tiene injerencia en todos los dominios (terrestre, marítimo, aéreo, espacial y del ciberespacio) y en el que operan

Objeto de la pregunta	Especialista	Información obtenida
		capacidades militares muy disímiles entre sí. Además de que el contexto actual impone hacer frente a diferentes áreas de misión y ejecutar Operaciones Militares de guerra y distintas a la guerra. Finalmente, el conductor militar en este nivel interactúa con actores de distintas funciones, ámbitos y sectores.
	CRL BURBANO	- Mantener la capacidad necesaria para neutralizar amenazas internas, externas o hibridas. - Proyectar el ejército del futuro, con menos recursos, pero con más exigencias y más amenazas. - La formación de líderes multi-misión, capaces de enfrentar ambientes VICA (volátiles, inciertos complejos y ambiguos) que encajen en equipos de trabajo modulares de acuerdo con la misión a desarrollar.
	SR. DÍAZ DE V.	Es un entorno hostil, complejo e interconectado, (10:41) con entornos híbridos, con "armas cibernéticas" con capacidad de destrucción de sus capitales de información para afectar la toma de decisiones. (11:29).
¿cómo definiría el problema estratégico?	GDD GRIFFITHS	Es un problema de múltiples variables, es necesario entender la esencia del nivel estratégico y entender que la fuerza militar se emplea en un ambiente de fricción. Ese contexto del nivel estratégico tiene componentes de complejidad y de alta incertidumbre. Aplican para este nivel los escenarios VUCA[19] más lo disruptivo.
	GDD. PINO	Es un problema multifactorial de múltiples variables. Está de acuerdo con el concepto establecido por el autor.
	GDD. VARELA	Conforme a nuestra doctrina, es aquel del ámbito del JEMCO y que debe articular los medios de la Defensa Nacional, proponer los modos para poder dar cumplimiento a los fines del escalón político.
	GDB. GREZ	En la realidad nacional, como un problema que debe articular el empleo del poder militar para alcanzar los objetivos del poder político.
	CRL. VERA	Problema de la alta dirección y toma de decisiones que debe buscar contar con las capacidades necesarias para dar respuesta a los objetivos que se le plantean.
	TCL. VILLARROEL	Es más complejo, debido a que son múltiples las variables que impactan en el problema, difíciles de integrar, en el que puede presentarse un alto volumen de información, con carencia de herramientas de procesamiento de datos y con tiempos limitados. Por otra parte, son problemas de una estructura sin una solución única, simple o que permita asegurar que este sea resuelto, pudiendo hacer frente con COAs diversos y variados. Por lo

[19] VUCA, sigla utilizada para concentrar los términos de *Volatilidad, Incertidumbre, Complejo* y *Ambiguo.*

Objeto de la pregunta	Especialista	Información obtenida
		anterior, **podría aseverarse que el problema estratégico es complejo y mal estructurado.**
	CRL. BURBANO	Su resolución no tiene una formula militar por sí sola, requiere integración de esfuerzos, agencias y recursos, acompañada de una decisiva voluntad política. La repetición de resultados táctico-operacionales contribuyen a un logro estratégico.
	SR. DIAZ DE V.	Como una situación que posee una superficie de exposición a las naciones y los estados cada vez mayor (08:32), se dan condiciones que relacionadas entre sí son muchas más complejas y sinérgicas. Que actualmente las capacidades de influencia en el ciberespacio son inconmensurables, por lo que el problema de este nivel no tiene solución predecible.

Nota: Tabla elaborada por el autor.

Conforme a lo anterior ha sido posible rescatar información desde dos puntos de vista que vienen a validar y contribuir el concepto de *Problema Estratégico* desarrollado en el presente capítulo.

Por una parte, y como objeto de la primera pregunta de la entrevista respecto a las características del problema militar estratégico, existió una cierta aprehensión a utilizar los conceptos referidos a la estructuración de este (bien o mal estructurado), pero lo que si se reafirmó, conforme a lo investigado previamente, es que quedaron de manifiesto los conceptos de complejidad, multiplicidad de variables o factores, incertidumbre y dinamismo, así mismo, como la congruencia de opinión respecto a que su comprensión permitirá dar respuesta al objetivo político planteado, asumiendo que en la mayoría de las veces excederá a lo netamente militar, lo que permitió reforzar la inferencia que este problema necesita una metodología de análisis de comprensión del ambiente estratégico, que considere una mayor cantidad de variables.

Del mismo modo, y desde una perspectiva mas desafiante para los entrevistados, se intentó obtener una definición propia respecto al problema estratégico, en la mayoría de los casos se les presentó el concepto acuñado por el autor de la investigación, obteniendo respuestas más cerradas concordantes con lo planteado, pero el hallazgo más importante que permitió esta interpelación, fue identificar puntos de vista diversos de cómo se comprende la estrategia, rescatándose los siguientes puntos:

- Los cuatro oficiales generales, tres de ellos integrantes actuales o en el pasado del Comité Estratégico del Ejército, aglutinaron el concepto en el nivel estratégico de la conducción, su indisoluble relación con los objetivos políticos y la aceptación del concepto acuñado por el autor.

- Los coroneles Burbano y Vera desde su perspectiva, lo abordaron desde el punto de vista del desarrollo de capacidades y la voluntad política asociada al empleo de estas capacidades, y, por último,

- El Tcl. Villarroel reforzó los conceptos de la complejidad y dificultad en su determinación o estructuración, mientras que el Sr. Díaz de Valdés combinó la complejidad del entorno estratégico con las capacidades asociadas al ciberespacio.

De todo lo anterior, se pudo reafirmar que los antecedentes presentados en las diferentes doctrinas analizadas, así como textos de publicaciones oficial de escuelas de guerra o estudios estratégicos están, en directa concordancia con las experiencias de los especialistas entrevistados, no habiendo unidad de criterios, pero si una convivencia de los conceptos desarrollados, lo que ha hecho factible reafirmar que el término acuñado para el *problema estratégico,* está en armonía doctrinaria y de praxis, quedando a firme como marco para el contexto de la investigación.

2.7 Síntesis del capítulo

El propósito del capítulo fue determinar qué se entiende por *problema estratégico*, a través de una metodología que involucró la descomposición del tópico conforme al marco establecido para el *nivel estratégico de la conducción militar*. Es así como tras la indagación en diferentes doctrinas y publicaciones afines, en un primer momento se abordó el problema militar y cuáles son las características del más alto nivel de la conducción, obteniéndose como resultado una serie de adjetivos calificativos los cuales fueron agrupados en los conceptos más significativos como *complejos, inciertos, dinámicos e interdependientes.*

En un segundo momento, se acotó claramente que significa el *nivel estratégico* para cada una de las perspectivas analizadas, siendo un trabajo de indagación principalmente en las doctrinas del ámbito conjunto, para lograr tener un parangón con la realidad nacional. Producto de este análisis, fue posible determinar que existen elementos comunes para este nivel como por ejemplo; la concentración de todas las fuerzas armadas o militares de una nación bajo un mando centralizado, que su planificación obedece a las necesidades del poder político a través de la demanda de opciones de respuesta militar en pos de un objetivo político, y por último, que se utilizan metodologías de análisis especiales y diferentes a las que se pueden usar en los niveles inferiores de la conducción debido a las características del problema que se les presenta.

Por último y una vez terminado el análisis de las diferentes perspectivas (doctrinarias y especialistas) tanto del nivel estratégico, como del problema militar, se acuñó una definición que se adoptó como marco para el resto de la investigación, sirviendo como punto de partida para iniciar la indagación de las características de la Ciberdefensa y sus alcances.

CAPÍTULO III
EL 5TO DOMINIO DE LA GUERRA Y LA CIBERDEFENSA

3.1 Metodología del capítulo

El presente capítulo ha buscado contestar la interrogante acerca de cuáles son las características estructurales de la Ciberdefensa en las naciones referentes, claramente condicionadas por las características reinantes en el *ciberespacio* o también denominado *5to dominio de la guerra*. Al igual que el capítulo anterior la metodología se basó en la indagación de diferentes fuentes de información nacionales y extranjeras (manteniendo como fuentes prioritarias aquellas de Colombia, España, Estados Unidos y Reino Unido), así como la opinión vertida por entrevistados relacionados con el área de estudio. Para este caso en particular, ha sido necesario ampliar algunos conceptos estampados en las respectivas doctrinas, a través de estudios y publicaciones afines con el tópico de la *Ciberdefensa*, escritos que generaron información valiosa para la investigación, en consideración a la constante evolución del concepto en estudio.

En primer término, se hace presente que la definición de *Ciberespacio o 5to dominio de la guerra* no es objeto de este capítulo, ya que no solo se han descrito sus alcances en el capítulo primero, sino que además se ha construido el concepto que dio marco a la presente investigación. Indistintamente de lo anterior, han sido desarrolladas y ampliadas algunas ideas, así como, mencionadas las particularidades reinantes, para poder describir posteriormente, las características de la Ciberdefensa en estructura y alcance.

En segundo término, se vuelve a recalcar que, para las definiciones específicas de *Ciberespacio* y *Ciberdefensa*, no existe un consenso académico, por lo que, a través de la exploración bibliográfica y perspectivas de especialistas, se buscó precisar las *características estructurales de la Ciberdefensa* que han permitido situarla como un *problema estratégico* conforme a la definición plasmada en el capítulo segundo.

Por último, se reitera que, desde el punto de vista de la doctrina, el marco de consulta ha sido aquel de la Doctrina Nacional Conjunta o sus homólogos en doctrinas extranjeras, siendo además otras fuentes útiles, las respectivas doctrinas institucionales. Lo anterior se señala en caso de existir vacíos u obsolescencia de alguno de los textos antes mencionados.

3.2 Aproximación teórica del concepto

En el capítulo anterior se ha logrado definir qué se entiende por *problema estratégico,* concepto que ha aportado el marco general para esta investigación y poder, al término de ella, establecer por qué la Ciberdefensa es un problema del nivel estratégico de la conducción. Para lograr lo anterior, se planteó que era necesario conocer y describir cuáles son las características estructurales de la Ciberdefensa, enmarcadas en el *5to dominio de la guerra* o *ciberespacio*. Conforme a lo anterior, ha sido preciso señalar que para este trabajo académico el *ciberespacio* se entiende como: *el entorno físico y abstracto que se desenvuelve en el ambiente de la información e involucra las plataformas, capitales de información y las relaciones e interacciones sociales que tienen lugar en este*[20].

Habiendo refrescado el concepto de cómo ha sido entendido el ciberespacio, es preciso señalar, que su acepción como *5to dominio*, deviene de la clasificación militar, para explicitar los espacios o lugares en donde pueden acaecer operaciones militares, y que en el transcurso de la historia han variado en la medida que los ingenios tecnológicos han permitido ampliar el uso de las capacidades militares en otros espacios, sumando a los dominios tradicionales conocidos hasta el siglo XIX de la tierra y el mar. A partir de la Primera Guerra Mundial y en los conflictos posteriores, se han adicionado los dominios como el aire y el espacio, para finalmente a fines del siglo XX incorporar el ciberespacio. Para precisar lo anterior es que la DNC 2-11 *"Doctrina Conjunta de Ciberdefensa"* (2018) establece que el concepto de *dominio* debe ser entendido como *"… un término empleado para referirse al medioambiente físico o virtual con características propias en las que se realizan actividades humanas:*

[20] Definición acotada por el autor.

marítimo, terrestre, aéreo, espacial y ciberespacial" (Ministerio de Defensa Nacional, 2018. p:30).

Complementando lo anterior, la misma publicación citada en el párrafo precedente plantea que, al mencionar el ciberespacio se debe tener presente que, en él no aplican todos los conceptos propios de los espacios tangibles, por lo que al hablar de *"… continuidad territorial, distancia, control del espacio de batalla, etc.… en el ciberespacio estas se vuelven irrelevantes"* (Ministerio de Defensa Nacional, 2018. p:7). Lo anterior entrega un marco claro que viene a dar ciertas libertades a las acciones que en este dominio existen, encontrándose pocas o ninguna limitante desde el punto de vista espacial.

Para dar mayor profundidad a lo descrito y ampliar la comprensión del concepto, el Crl. Marcelo Masalleras en su artículo *"Seguridad y ciberseguridad: precisiones de una tarea compartida"* establece claramente que desde el momento en que se pueden *"…identificar riesgos y amenazas provenientes del ciberespacio, tanto para gobiernos, instituciones y las personas, es que debe considerarse como quinto dominio"* (Masalleras, 2021. p:4), entendiendo en el mismo artículo, que los dominios tradicionales son la tierra, el mar, el aire y el espacio, donde debe ser reconocido el *ciberespacio* como el 5to dominio.

Por su parte el Ejército de Chile en su reglamento de doctrina *"La Fuerza Terrestre"* establece que para la definición de un *Ambiente Operacional* es necesario entender todas aquellas características *"…que afectan el empleo de las capacidades en todos los dominios (terrestre, marítimo, aéreo, espacial y ciberespacio)…"* (Ejército de Chile, 2019. P: 15). Si bien no hay una precisión o definición del 5to dominio, en otras publicaciones si detalla lo que se debe entender por ciberespacio, acotando el concepto de *dominio* solo al espacio físico y abstracto donde se emplea la fuerza militar.

Por otro lado, la Doctrina Conjunta citada dedica algunas páginas para establecer cuáles son las características del Ciberespacio, que deben ser tomadas en cuenta para la ejecución de acciones en este dominio por parte de la fuerza. Dentro de las

características que podemos encontrar se consideran las siguientes: 1) Discreto, 2) Dinámico, 3) A territorial, 4) Desregulado, 5) Anónimo, y 6) Privado. Considerando estas características fue posible, primero tener la referencia de las condiciones en las que se concibe la Ciberdefensa Nacional y, segundo un parámetro de comparación con las doctrinas y estudios de otros países.

Fuera del ámbito nacional, y buscando ampliar la comprensión del 5to dominio de la guerra, y como este viene a determinar las características de la Ciberdefensa, una gran cantidad de autores colombianos han tomado la vanguardia en el cono sur desde el año 2011[21], y se puede extraer de algunos de sus estudios ciertas particularidades del ciberespacio, que finalmente condicionarán la Ciberdefensa. Es así como el especialista en seguridad informática de la Universidad Piloto de Colombia, el Sr. Wilson Cárdenas Moreno, establece los siguientes *problemas del ciberespacio* en el contexto de Colombia: 1) debilidad en la normativa de los proveedores de internet, 2) los tiempos de conservación de evidencia para investigación forense no está regulada, 3) Débil sistema de identificación de actores, 4) Incremento de la impunidad, 5) Incremento del riesgo (por digitalización del Estado y por incremento de la ciberdelincuencia), y 6) Rezago del país frente a la comunidad internacional.

De todo lo anterior Cárdenas concluye que *"… con el fin de lograr los objetivos estratégicos, es necesario involucrar en el ciberespacio a instituciones del Estado con responsabilidades de Ciberseguridad y Ciberdefensa"* (Cárdenas, 2015. p:3), lo anterior viene como una proposición para dar una respuesta integrada a una serie de factores de riesgo desde el punto de vista del especialista.

Ampliando las ideas antes expuestas, en el caso español, fue factible identificar algunas características bien definidas del ciberespacio, que han sido declaradas por la *Escuela de Altos Estudios de la Defensa,* dependiente del Ministerio de Defensa de España, en donde se determina que este *dominio* debe entenderse como: 1) altamente dinámico; 2) costos de acceso irrelevantes; 3) alto nivel de crecimiento; 4) alta

[21] El año 2011 Colombia publica su primera Política de Ciberseguridad y Ciberdefensa, siendo el primer país latinoamericano con contar con una normativa, objetivos y alcances determinados a nivel gubernamental.

capacidad de procesamiento; 5) carácter asimétrico; 6) Anonimato; 7) producir efectos físicos y; 8) transversalidad de sus efectos. Además de lo anterior, establece que:

> En el ámbito particular de la defensa, tierra, mar, aire y espacio han sido los dominios tradicionales en los que se han desarrollado las operaciones militares y, por tanto, en los que se han focalizado los esfuerzos relacionados con la obtención de las capacidades militares. Sin embargo, el ciberespacio ya ha sido definido y aceptado como el quinto dominio, en el cual se llevarán a cabo operaciones militares específicas y que ya apoyan actualmente las operaciones militares que se desarrollan en el resto de los dominios. (Ministerio de Defensa de España, 2014. p: 16)

Las ideas vertidas en los párrafos anteriores han dejado de manifiesto que España, en el más alto nivel identifica características del ciberespacio y declara directamente que será considerado como un *dominio de la guerra*, desde donde se configurarán operaciones en apoyo al resto de los dominios.

Por otra parte, se ha podido analizar el caso de Estados Unidos que el año 2020, se situaba a la vanguardia de estudios y publicaciones asociadas al Ciberespacio y Ciberdefensa (Valencia, Patiño & Arenas, 2020 p:371), por tanto, su desarrollo ha marcado tendencia mundial con la contraposición solo de Rusia y China. El referente norteamericano, no solo posee el mayor número de publicaciones, sino que ya tiene consolidada la normativa y las estructuras asociadas al control y defensa de sus intereses en el ciberespacio. Desde el nivel estratégico (refiérase a la *Figura N.º6. p:36*), el mismo Secretario de Defensa, asume que la mayor cantidad de riesgos para los intereses de Estados Unidos, se encuentran plasmados en el 5to dominio, estableciendo *"…nuestros adversarios recurren cada vez más a actividades malignas en ámbitos menos tradicionales para socavar nuestra seguridad, ... Quizá no haya ningún área en el que esto sea más cierto que en el dominio cibernético" (*Esper, 2019).

Considerando la importancia que Estados Unidos entrega al *5to dominio*, es que hace énfasis en la identificación de las características de este ambiente, demostrado en el enfoque que le da el Departamento de Defensa (DoD), en un sentido militar

permanente. La publicación matriz es la JP 3-12 *"Cyberspace Operations"* y las publicaciones subsidiarias consideran la misma definición del ciberespacio, que en síntesis establecen que este es un *dominio* interno del ambiente de la información, que se extiende a través de las fronteras geográficas, el cuál es inherentemente *conjunto, interagencial y multinacional.*

Por último, la perspectiva del Reino Unido, al igual que las anteriores, ha considerado el ciberespacio como el 5to dominio de la guerra, asumiéndolo como un área nueva de riesgos para la nación conforme lo expresa Robert Bloomfield en su Tesis Doctoral *"Bullets to Bytes"* en estudios de conflictos modernos e historia militar contemporánea. La publicación establece que, solo desde el 2009 el Reino Unido ha asumido el riesgo del ciberespacio como una real amenaza, pero que rápidamente aquellos responsables de la elaboración de políticas y especialmente aquellos asociados a Defensa, han tomado cartas en el asunto, donde deja de manifiesto lo siguiente:

> …los responsables de la Defensa se esfuerzan por comprender y responder a los desafíos del ciberespacio como dominio de la guerra junto con el marítimo, el terrestre, el aéreo y el espacial. Un dominio de guerra tan nuevo que no fue reconocido oficialmente por la Organización del Tratado del Atlántico Norte (OTAN) hasta 2016. (Bloomfield, 2019. p:20).

Además de lo anterior, y a diferencia de lo planteado anteriormente, la publicación doctrinaria *"Operations"* del Ejército del Reino Unido, plantea que una de las características del ciberespacio es:

> …a diferencia de los dominios de la guerra física, el ciberespacio no tiene un componente ambiental y está presente en todas las operaciones que involucran a la tierra, el mar y el aire; por lo tanto, la responsabilidad de explotar su potencial y protegerse de sus amenazas es común a todos los componentes [de la defensa]. (Reino Unido, 2017. p:33)

Conforme a lo expuesto, respecto al Reino Unido, también queda de manifiesto que el ciberespacio es *el 5to dominio de la guerra*, donde se desarrollarán operaciones

militares en un ambiente con particularidades especiales y que son transversales a los dominios físicos.

La descripción conceptual plasmada en párrafos anteriores, no solo extraída de la doctrina, sino que además de publicaciones y estudios, ha permitido comprender el marco espacial en donde tiene cabida la Ciberdefensa, de esta manera se pudo, rápidamente, establecer que el ciberespacio es un ambiente donde se presentan riesgos y amenazas a los estados y las personas, que no respeta límites territoriales, ni las particularidades del factor espacial (distancia, geomorfología, etc.), y que es menester de los gobiernos y en especial del sector Defensa la acción de protección y disuasión de posibles amenazas a los intereses nacionales, que son susceptibles de ser afectados en este dominio. En adición a lo anterior, han surgido calificativos como dinámico, interagencial, multinacional, que le otorgan una complejidad mayor al desafío de la *Ciberdefensa* del Estado.

3.3 Características estructurales de la Ciberdefensa

Conforme al marco descrito en los capítulos anteriores y en el punto precedente, se ha podido complementar la definición del ciberespacio considerada para esta investigación, con algunas características del dominio. Además, se ha tenido a la vista la definición del *problema estratégico*, de tal forma que fue posible ir aproximando al objetivo principal de la presente investigación, que es establecer por qué la *Ciberdefensa* debe ser considerada como un problema de la conducción estratégica. Conforme a lo anterior, el próximo paso fue la determinación de características estructurales de la Ciberdefensa y cómo se concibe en el nivel nacional, así como en los países referentes seleccionados, haciéndose necesario no solo haber indagado en diferentes publicaciones doctrinarias, sino que además haber logrado inferencias por parte del autor, respecto a cuáles de ellas se aproximan más al nivel estratégico de la conducción en Chile.

3.3.1 Chile

Respecto a lo anterior se ha hecho énfasis que a nivel nacional existe la Política Nacional de Ciberdefensa del año 2018, la cual tiene cabida en dos áreas, la primera como parte de la Política de Defensa Nacional y la otra como parte de la Agenda Digital del Estado al año 2020. Consecuente con lo anterior, se ha emanado la respectiva publicación de la Doctrina Nacional Conjunta, DNC 2-11 *"Doctrina Conjunta de Ciberdefensa"* (2018). El preámbulo ha sido concebido para dejar de manifiesto que, como ejercicio académico, se ha tomado como pivote la doctrina y normativa nacional, siendo consideradas además como fuentes primarias, por lo que el análisis de otras doctrinas ha tenido la voluntad de comparar la congruencia en características estructurales, como por ejemplo: 1) Definición, 2) Propósito que busca, 3) Responsable y/o encuadramiento en el Estado, 4) Marco legal o regulatorio, 5) Principios o componentes que la rigen, y 6) Alcance (Fuerzas Armadas o Interagencial).

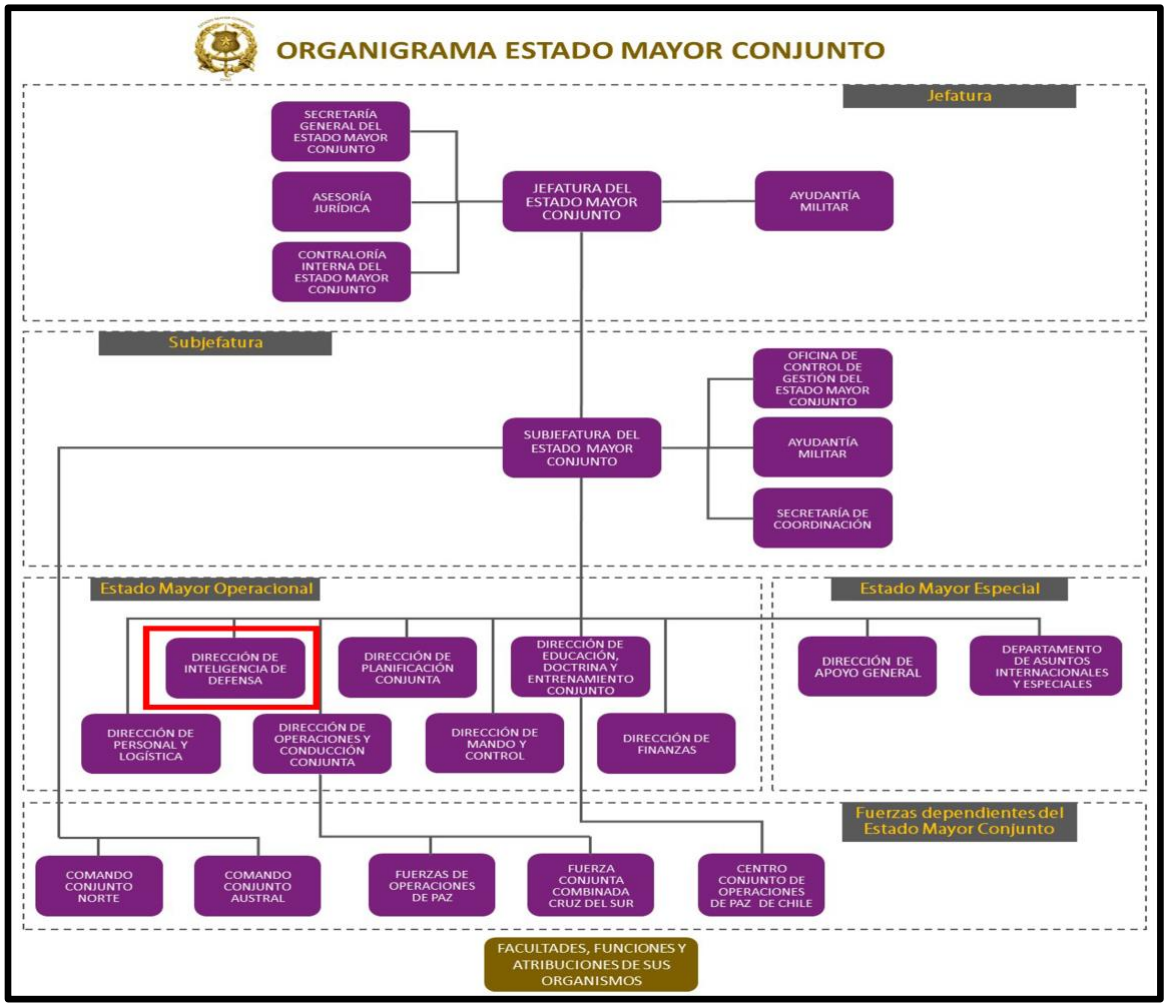
En las particularidades de la Política de Ciberdefensa de Chile, queda establecido que la Ciberdefensa debe ser entendida como *"Conjunto de principios, políticas e instrumentos destinados a proteger el ciberespacio desde un punto de vista de la defensa nacional y estratégico-militar"* (BCN, 2019. p:6) y por su parte la doctrina conjunta desarrolla la definición en dos núcleos conceptuales, primero establece que *"…Corresponde al conjunto de políticas y técnicas de la Defensa Nacional destinadas a enfrentar los riesgos y amenazas propias del ciberespacio de acuerdo a sus atribuciones constitucionales y legales"* (Ministerio de Defensa, 2018. p:14) y en la acepción específica establece que *"…es una actividad del ámbito de la Defensa Nacional, que apoya a las operaciones militares y enfrenta las acciones hostiles en el CE… la CDef se materializa mediante Ciberoperaciones que componen el empleo militar del CE…"* (Ministerio de Defensa, 2018. p:14).

De ambas definiciones anteriores, se obtuvieron elementos concretos como su vinculación al amplio espectro de la Defensa Nacional, que posee un componente normativo y legal, principios de empleo, y por último un componente ejecutivo de apoyo a las operaciones militares o empleo de la fuerza.

Respecto al objetivo o propósito de la Ciberdefensa que pudo ser identificado en la Política Nacional, establece que será, *proteger el ciberespacio desde el punto de vista de la Defensa Nacional y estratégico militar*, es decir, sus activos de información, infraestructuras críticas y redes. Todo lo anterior, ha permitido deducir que su alcance es en el ámbito de las FAs, aunque no ha sido posible ser taxativo respecto a este punto debido a la indisoluble cooperación con la Política Nacional de Ciberseguridad (PNCS), donde parte de las infraestructuras críticas del gobierno pueden ser del ámbito de la Defensa nacional, lo que le ha dado matices de interagencialidad, que vienen a confirmarse en la Política Nacional de Ciberdefensa (PNCD), la que expresa que *"La colaboración en el trabajo y acción en materias de Ciberdefensa se materializará de forma integral con otros sectores del país, con entidades privadas, y con la sociedad civil"* (Chile, 2018. p:5).

Para el caso chileno, la PNCD establece claramente que recaerá la responsabilidad en el Ministerio de Defensa Nacional, la articulación de planificación, organización y ejecución de la Ciberdefensa donde se puede destacar lo siguiente *"La Ciberdefensa ha impuesto retos que deben ser afrontados institucionalmente. Para ello, la Defensa Nacional realizará la reorganización orgánica que sea necesaria para el cumplimiento de sus funciones en el ciberespacio, que comprenda, al menos… se creará un Comando Conjunto de Ciberdefensa, bajo el mando del Jefe del Estado Mayor Conjunto, responsable del planeamiento y ejecución de las operaciones militares conjuntas de Ciberdefensa del país"* (Ministerio de Defensa Nacional, 2018. p:5). En base a lo anterior, no queda de manifiesto en la PNCD que hay un organismo específico para encuadrar a la Ciberdefensa, sino que se debe crear un Comando Conjunto que cuente con las capacidades, aun cuando la realidad, es que desde que se publicó la PNCD el 2018, el EMCO accionó en forma inmediata, creando la unidad de Ciberdefensa encuadrada en la Dirección de Inteligencia de la Defensa, homologando los encuadramientos que las instituciones de las FAs habían propiciado para sus unidades de Ciberdefensa, debido a la posibilidad de encuadrar y legitimar algunas de las operaciones en el ciberespacio bajo el amparo de la Ley 19.974.

FIGURA 9 Encuadramiento de la Ciberdefensa en el Organigrama de la Jefatura del Estado Mayor Conjunto de Chile



Nota: "Encuadramiento de la Ciberdefensa en el Organigrama de la Jefatura del Estado Mayor Conjunto de Chile". Figura obtenida por el autor a partir del Organigrama de la dicha Jefatura, (Ministerio de Defensa Nacional, 2022).

Como último punto, desde la perspectiva de Chile, la DNC 2018 ha estimado pertinente decretar que la Ciberdefensa se deberá regir en sus bases por tres principios normativos, que le permitirán tener una guía clara sin necesariamente caer en el pragmatismo, estos principios son la *inteligencia*; la *tecnología* y la *cooperación*. El primero de ellos respecto a la comprensión de las amenazas y el ambiente operacional; el segundo respecto a la modernización permanente y; el tercero respecto a los flujos de información e inteligencia con otras agencias de las instituciones armadas o el Estado.

3.3.2 Colombia

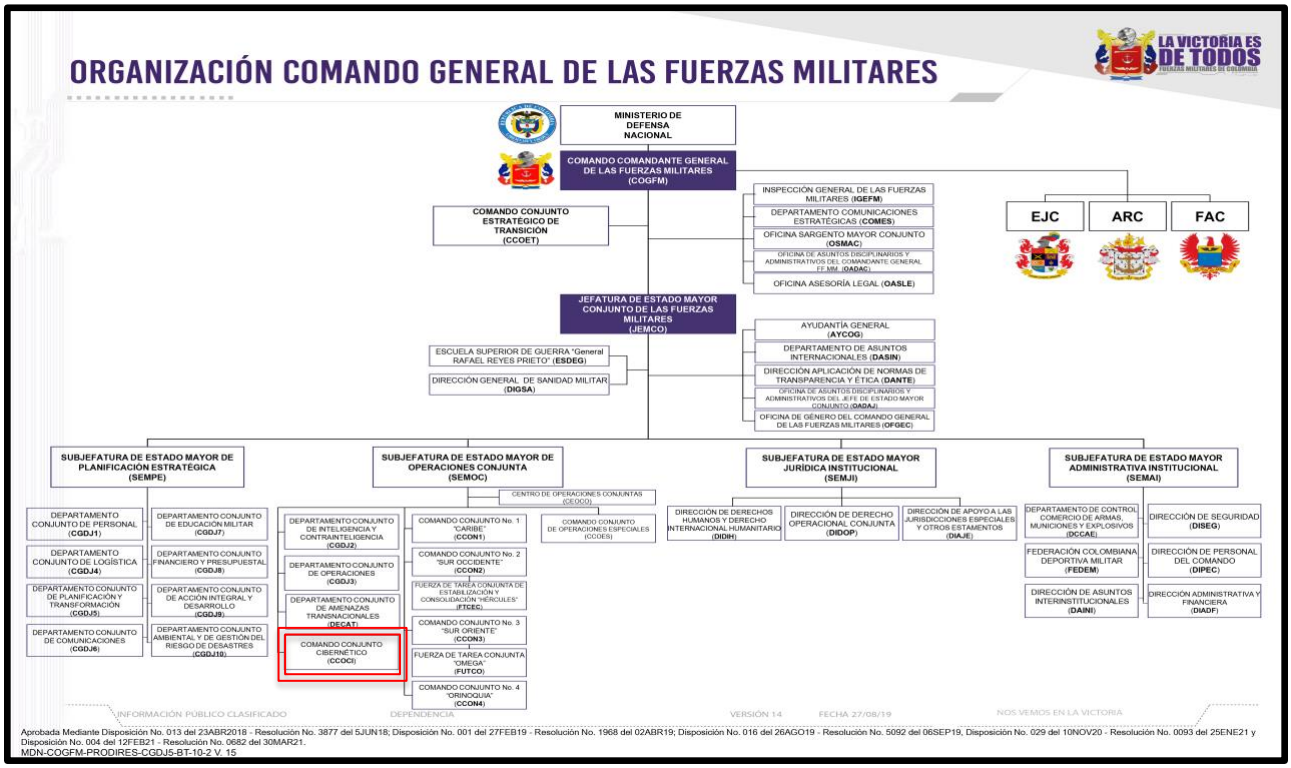
Desde la perspectiva colombiana, la Ciberdefensa viene tratada con algunas particularidades respecto a Chile, primero que todo, en la definición específica que otorgan las Fuerzas Militares y el Ejército Nacional de Colombia, es posible destacar lo siguiente:

> Las acciones que lleva a cabo el Estado para proteger y controlar los posibles riesgos cibernéticos, con el objetivo de poder hacer uso del ciberespacio con tranquilidad, protegiendo de igual manera la integridad del territorio. La ejecución de la Ciberdefensa está al mando de las Fuerzas Armadas, quienes protegen las infraestructuras críticas del Estado… siendo la capacidad del Estado para prevenir y neutralizar las amenazas cibernéticas que afectan la soberanía, esta defensa es tanto activa como pasiva de todo el ciberespacio, donde se protege la información institucional y se resiste contra los ciberataques, su principal arma es la comunicación militar que protege de esta manera la infraestructura crítica del país, según lo presentado por las Fuerzas Militares de Colombia. (FF.MM. y Ejército Nacional, 2015, p:4).

La definición anterior permite identificar que está claramente enmarcada en el ámbito militar, con responsabilidades genéricas al sector Defensa. Por su parte el propósito, aun cuando no está declarado explícitamente en la misma definición, otro autor expresa que: *"se centra en la fase operativa de los ciberataques y desarrollar la defensa y protección de las redes e infraestructura crítica de la Nación"* (Villanueva, 2018).

Por otro lado, Colombia aborda este tópico en el año 2011 en el Consejo Nacional de Política Económica y Social (CONPES), donde se delinea la Estrategia de Ciberdefensa y se establece la creación de la Política de Ciberseguridad y Ciberdefensa. Este hecho deja claramente establecido que, para los intereses de Colombia, debía obedecer a una estructura interagencial compuesta por el Equipo de Respuesta de Incidentes de Colombia (ColCERT); el Centro Cibernético Policial (CCP) y el Comando Conjunto Cibernético (CCC) dependiente exclusivamente de las Fuerzas Armadas (Gómez; Luciano & Carlos, 2020). *Figura N.º10*.

FIGURA 10 Encuadramiento del Comando Conjunto Cibernético, en la organización del CGFA



Nota: Figura obtenida por el autor a partir del organigrama del Comando General de las Fuerzas Armadas de Colombia, (Colombia, 2022).

Desde el punto de vista de los componentes estructurales o principios que guían, fue posible identificarlos y posee un número mayor de factores (respecto a Chile) que le dan una amplitud superior. Dentro de los componentes estructurales la *"…Ciberdefensa se caracteriza por seis componentes principales en los que las Fuerzas Militares de Colombia han soportado el desarrollo de capacidades de Ciberdefensa y su fortalecimiento*." Donde fue posible identificar los siguientes: 1) Personas, 2) Procesos, 3) Tecnología, 4) Cooperación, 5) Operaciones, y 6) Marco Legal. (Villanueva, 2018). Cada uno de esos componentes son desarrollados al detalle con el fin de dar el marco mínimo indispensable para el sustento de la *Ciberdefensa.*

Por último y desde la mirada de la amplitud y/o alcances de la Ciberdefensa en Colombia, fue posible afirmar que es Interagencial desde sus orígenes legales, puesto que la Política Nacional no hace diferencia jerárquica entre Ciberseguridad y Ciberdefensa como pasa en Chile, dando un marco claro de desarrollo sin tipificarla

como un problema aislado. Lo anterior, tiene sustento en lo establecido en su Política de Defensa como sigue: *"será responsabilidad de todas las instituciones Públicas y Privadas, dar cumplimiento a las políticas públicas y a los planes intersectoriales para el control y prevención de ciberataques y ciberdelitos, siendo su principal responsabilidad, la de elaborar y mantener actualizados los planes de seguridad y defensa, para garantizar la Ciberseguridad y Ciberdefensa de la Nación"* (Colombia, 2020. p:28).

3.3.3 España

Para el resto de los países referentes utilizados en la presente investigación, a pesar de ser todos integrantes de la OTAN, cada uno de ellos define la *Ciberdefensa* en forma particular y a nivel *Conjunto*, donde ha sido posible identificar las características estructurales de cada uno de ellos. Es así, como España en su *Nivel Conjunto* define *Ciberdefensa* como el;

> Conjunto de capacidades de defensa, explotación y ataque que permiten llevar a cabo operaciones en el ciberespacio, con la finalidad de preservar o ganar la libertad de acción en el ciberespacio de interés militar, impedir o dificultar su uso por parte del adversario, y contribuir a alcanzar la superioridad en el enfrentamiento en el resto de los ámbitos físicos y cognitivo. (España, 2020. p:20)

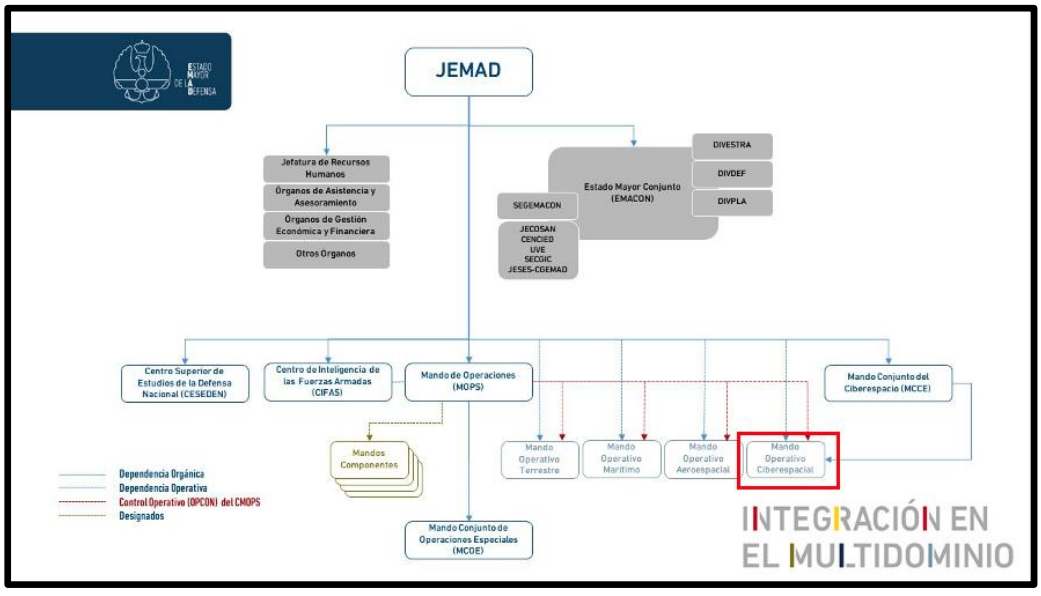
Cabe destacar que España, como parte de su arquitectura gubernamental y específicamente para el Ministerio de Defensa, posee bajo su mando al Estado Mayor de la Defensa (EMAD), quien cuenta con una organización específica para la planificación y conducción de las acciones en el ciberespacio, este es el *Mando Conjunto del Ciber Espacio* (MCCE), es así como ha sido posible establecer que la responsabilidad de la *Ciberdefensa* recae directamente en el Comandante del Comando Conjunto del Ciberespacio, y este a su vez depende del EMAD. (España, 2021).

Desde el punto de vista del marco legal, es posible destacar algunas cosas diferenciadoras a las dos realidades antes analizadas. Para España, existe el marco regulador del gobierno, desde donde se desprenden las responsabilidades de la

Constitución Española de 1978, seguido de lo anterior, emanan las Políticas y Estrategia de Seguridad Nacional, donde viene enmarcada la Estrategia Nacional de Ciberseguridad (2019), a simple vista no difiere respecto a lo de Chile, excepto por que es más amplio y no se circunscribe a una ley de inteligencia, por ejemplo.

El real aspecto diferenciador para el marco legal de España es que, como miembro de la OTAN, adhiere a lo establecido en *Manual de Tallin*[22], donde existe la posibilidad de tipificar jurídicamente y asimilar los ciberataques a aquellos ataques armados convencionales (Amich, Velásquez. 2014). Debido a lo anterior, es que para España y, será lo mismo para Reino Unido, existen tanto restricciones como garantías para el uso de la fuerza militar en el ciberespacio a nivel nacional como miembros de la alianza.

FIGURA 11 Encuadramiento del Mando Operativo Ciberespacial, en la organización del JEMAD



Nota: Figura obtenida por el autor a partir del organigrama del Jefe del Estado Mayor de la Defensa de España. (España, 2022).

[22] Manual de Tallin, es un estudio académico de la aplicabilidad del Derecho Internacional en los conflictos en el ciberespacio, al cuál han adherido la mayoría de países de la OTAN y por los que rigen su actuar. No constituye un tratado, no obstante sirve como marco regulatorio para la Alianza.

Respecto a los componentes que rigen la Ciberdefensa o bien sus principios fundamentales, España los ha definido en su *Concepto de Ciberdefensa,* publicación del Ministerio de Defensa español, de septiembre de 2018, donde establece que los componentes centrales son: 1) Terminología Común, 2) Capacidades de Ciberdefensa, 3) Operaciones en el ciberespacio, 4) Integración a operaciones conjuntas, 5) Marco Legal, 6) Estructura de mando y control, 7) Integración Interagencial e Internacional, 8) Capacitación e Idoneidad del Personal, 9) Inversión, desarrollo e innovación (I+D+i). (España, 2018).

Por último, y respecto a los alcances de la Ciberdefensa, ha sido posible evidenciar en la investigación que al igual que Chile y Colombia, posee una connotación Interagencial, esto pudo ser evidenciado en las *Líneas de Acción* (LA) de la Estrategia de Ciberseguridad Nacional, donde la primera LA consiste en "*Incrementar las capacidades de prevención, defensa, detección, análisis, respuesta, recuperación y coordinación ante las ciberamenazas, haciendo énfasis en las Administraciones Públicas, las Infraestructuras Críticas, las capacidades militares y de Defensa y otros sistemas de interés nacional"* (España, 2013. p:31).

3.3.4 Estados Unidos

Este país ha sido un actor interesante de analizar pues posee una arquitectura diversa para encuadrar el accionar de la *Ciberdefensa*, puesto que el término, hace referencia a la *defensa del ciberespacio* como una operación específica dentro de la estructura superior de las *ciberoperaciones*, como sigue:

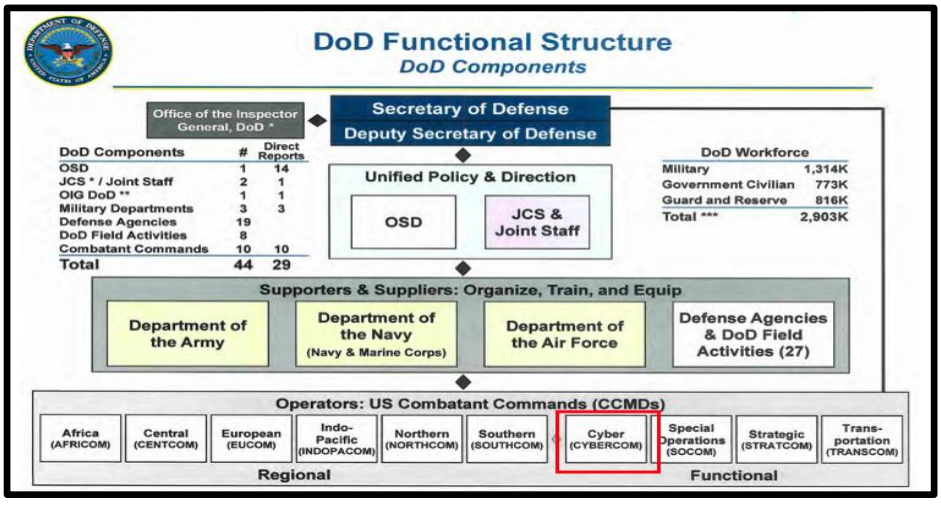
> Defensa del ciberespacio: Las acciones de defensa del ciberespacio se llevan a cabo dentro del ciberespacio protegido (soberano), para derrotar amenazas específicas que han violado o amenazan con violar las medidas de seguridad del ciberespacio e incluyen acciones para detectar, caracterizar, contrarrestar y mitigar las amenazas, incluyendo el malware o las actividades no autorizadas de los usuarios, y para restaurar el sistema a una configuración segura[23]. (Estados Unidos, 2018. p:40)

[23] Traducción hecha por el autor.

Independiente de lo anterior, abarca menos aristas que las consideraciones de Chile, Colombia y España. Al indagar acerca del propósito de esta, ha sido planteado en forma genérica para el concepto de *ciberoperaciones*, el cuál incluye la *defensa del ciberespacio*, y considera que *"el propósito principal es lograr objetivos en o a través del ciberespacio"*[24] (Estados Unidos, 2018. p:9). Lo anterior, que abiertamente, es de gran amplitud de interpretación, se hace pertinente e incluso lógico, en consideración a las condiciones del ciberespacio ya descritas, referido a que entrega libertad de acción a los comandantes.

Así como fueron descritas las particularidades de los niveles de la conducción para Estados Unidos, la arquitectura de Defensa presenta características estructurales particulares para el encuadramiento de la *Ciberdefensa*. Primero que todo, la *Ciberdefensa* en este caso se encuentra bajo el concepto de *ciberoperaciones*, estas están bajo la dependencia del *Comando Ciberoperaciones* (USCYBERCOM), el cual está enmarcado dentro de los Comandos Combatientes Funcionales, dependientes del *Departamento de Defensa* (DoD), y este a su vez depende del *Secretario de Defensa* (SECDEF) (Estados Unidos, 2022). Refiérase a Fig. N.º12.

FIGURA 12 Encuadramiento del Comando Ciberespacial, en la organización del DoD



Nota: Figura obtenida por el autor a partir del organigrama del Departamento de Defensa de los Estados Unidos. (Estados Unidos, 2022).

[24] *Ídem*.

Respecto de lo anterior, es factible establecer que la dependencia de la *Ciberdefensa* está al más alto nivel de la conducción puesto que se encuentra a la par con los otros Comandos Combatientes, dependientes del Departamento de Defensa y Secretario de Defensa del país.

Respecto al marco regulatorio que contiene a la *Ciberdefensa*, el caso de Estados Unidos es bastante explícito en su publicación doctrinaria *"Cyberespace Operations"* JP 3-12 del año 2018, que dedica un acápite a las consideraciones legales y establece entre otras cosas:

> El DoD lleva a cabo las ciberoperaciones de acuerdo con la legislación nacional de EE.UU., el derecho internacional aplicable y las políticas pertinentes del Gobierno de EE.UU. y del Departamento de Defensa. Las leyes que regulan las acciones militares en el territorio estadounidense también se aplican al ciberespacio. Por lo tanto, las fuerzas del ciberespacio del DOD que operan fuera del DODIN [25], cuando están debidamente autorizadas, a menos que se les emitan reglas de enfrentamiento diferentes o que realicen apoyo de defensa a las autoridades civiles (DSCA[26]) bajo la autoridad apropiada. (Estados Unidos, 2018. p:16)

Respecto al parámetro seleccionado de los *principios* normativos o elementos esenciales que rigen la *Ciberdefensa* o bien las *ciberoperaciones*, no fue posible identificarlos en la *"Cyber Strategy"*, pero sí en la doctrina conjunta asociada. Cabe destacar que al hablar de principios en el nivel del *CYBERCOM*, las referencias del JP 3-12, vienen asociadas a:

> las relaciones que deben mantener las ciberoperaciones con otras operaciones militares, tanto en planificación como en ejecución, van a afectar directamente a las fuerzas en los dominios netamente físicos, afectando en lo sustancial a los principios del empleo conjunto asociados a las ciberoperaciones que son la simplicidad, la agilidad y la economía de fuerzas. (Estados Unidos, 2018. p:27)

[25] DODIN, *Deparmet of Defense Informations Networks*. Departamento de Defensa de las Redes de Informaciones.
[26] DSCA, *Defense Support of Civileans Authorities*. Apoyo de Defensa a las Autoridades Civiles.

Lo anterior permitió deducir que las ciberoperaciones y la *Ciberdefensa* se rigen por los mismo *principios del empleo conjunto*, similares a los *Principios de la Guerra Conjuntos* de la Doctrina Nacional.

Por último, los alcances de la Ciberdefensa para los Estados Unidos, al igual que el marco regulatorio, vienen expresados tácitamente en el JP 3-12, que dentro de múltiples desafíos que posee la *Fuerza Conjunta para el uso del ciberespacio*, son las relaciones con la industria privada, la infraestructura pública, políticas interagenciales, entre otras. (Estados Unidos, 2018). Además de las características y necesidades interagenciales, como parte de la OTAN y otras posibles coaliciones, el mismo texto doctrinario, menciona los alcances *internacionales, multinacionales y coaliciones.*

3.3.5 Reino Unido

El último caso analizado es el Reino Unido, el cuál presentó ciertas dificultades en la búsqueda de definiciones específicas de lo que se entiende por *Ciberdefensa*, así mismo en la determinación exacta del encuadramiento de ella, debido a la complejidad que presentan algunas organizaciones, a manera de ver del autor, ya que se hallaron elementos dependientes del sector Defensa, así como interagenciales, *Ciberseguridad Nacional* y aquellos coaligados con la OTAN.

La definición de *Ciberdefensa* más precisa y aceptada por el Reino Unido se encuentra en la *Doctrina de Ciberoperaciones de la OTAN* AJP 3-20 del año 2020, que establece sucintamente que son aquellas *"acciones defensivas en o a través del ciberespacio para preservar la libertad de acción amiga en el ciberespacio"*[27] (OTAN, 2020. p:24). Evidentemente el tratamiento que el Reino Unido da al concepto es enmarcado en las ciberoperaciones al igual que los Estados Unidos. Así mismo el propósito que busca la *Ciberdefensa* será *"preservar la libertad de acción amiga en el ciberespacio y/o crear efectos para lograr los objetivos de los comandantes"* (OTAN, 2020. p:36). Tanto la definición anterior como el propósito que busca, fueron aquellos extraídos de la doctrina de la OTAN y confrontados con aquellos del sector Defensa, los cuáles son descritos a continuación.

[27] Traducción realizada por el autor.

La *Ciberdefensa* en los términos del estudio, para este caso particular, dependía hasta el año 2019 del *Comando de Fuerzas Conjuntas,* pero a partir de ese año se reestructuró bajo la denominación de *Comando Estratégico.* Este Comando es el responsable de asegurar que el *Ministerio de Defensa* cuente con la asesoría, planificación y conducción de las acciones conjuntas, como lo define el mismo Comando Estratégico: *"Apoyamos al Ministerio de Defensa (MOD), asegurándonos de que las capacidades conjuntas, como los servicios médicos, la formación y la educación, la inteligencia y los sistemas de información, se desarrollen y gestionen en los 5 dominios terrestres, marítimos, aéreos, espaciales y cibernéticos. También gestionamos las operaciones conjuntas en el extranjero"*[28]*.* (Reino Unido, 2022). (Referirse a *Figura N.º13 p:64).*

Este Comando está compuesto por ocho organizaciones, dentro de las cuáles se encuentra enmarcada la *Ciberdefensa,* por un lado, la organización directiva reconocida como *Defence Digital*, que tiene la misión de coordinar las *ciberoperaciones defensivas* para el Reino Unido, además apoyar la coordinación general y coherencia de todas las tecnologías de la información del Ministerio de Defensa. Por el otro lado, se encuentra la unidad ejecutiva identificada como *National Cyber Force*, que *"es responsable de operar en y a través del ciberespacio para contrarrestar, interrumpir, degradar y rebatir a aquellos que podrían hacer daño al Reino Unido o a sus aliados"*[29] (Reino Unido, 2022. p:42).

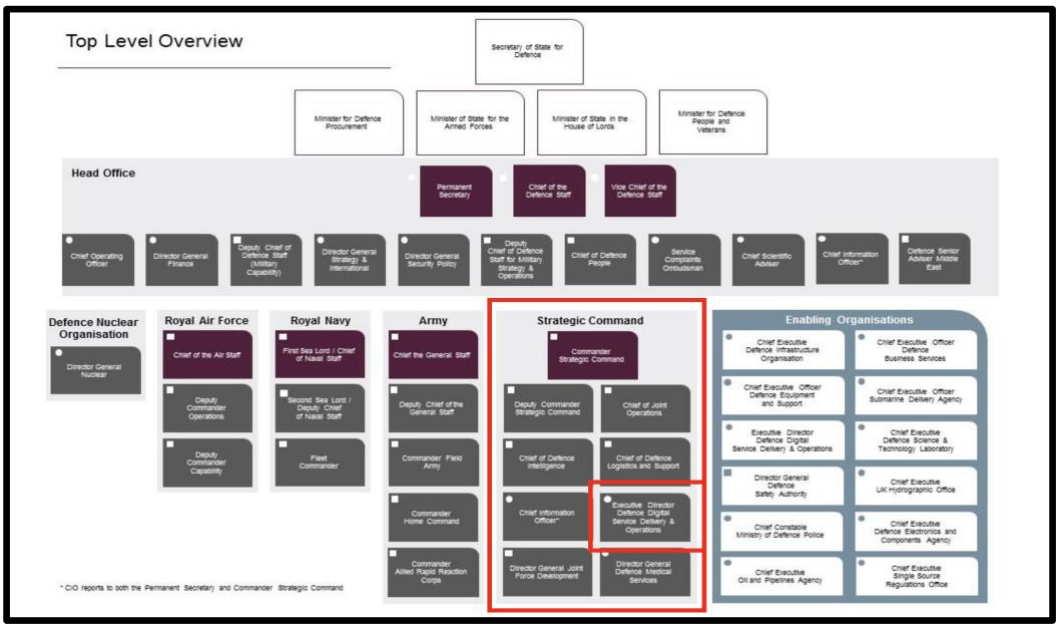
Desde el punto de vista del marco regulatorio, al igual que los Estados Unidos, está claramente definido en la Estrategia Nacional de Ciber donde explicita lo siguiente:

> Las operaciones se llevan a cabo de acuerdo con un marco legal bien establecido, que incluye la Ley de Servicios de Inteligencia de 1994 y la Ley de Poderes de Investigación de 2016. El Reino Unido ya ha dejado claro que desarrolla y despliega capacidades de acuerdo con el Derecho Internacional, incluido el Derecho de los Conflictos Armados cuando sea aplicable. Sus actividades están sujetas a la aprobación ministerial, la supervisión judicial y

[28] Traducción realizada por el autor desde sitio de internet, vínculo en acápite "Referencias".
[29] *Ídem*.

la revisión parlamentaria, lo que hace que el régimen de gobernanza del Reino Unido para las operaciones cibernéticas sea uno de los más sólidos del mundo[30]. (Reino Unido, 2022. p:42).

FIGURA 13 Encuadramiento del Comando Estratégico y Defensa Digital, en la organización del MOD



Nota: Figura obtenida por el autor a partir del organigrama del Ministerio de Defensa del Reino Unido. (Reino Unido, 2020).

Desde el punto de vista de los principios de empleo o estructurales, nuevamente aparecen principios de empleo conjuntos definidos en la AJP 3-20, lo que tiene toda lógica por la manera en que se encuadra y conceptualiza la Ciberdefensa en el Reino Unido, pudiéndose destacar los siguientes: 1) Seguridad, 2) Sorpresa, 3) Concentración de Fuerza, 4) Mantención de la moral, y 5) Libertad de acción.

Por último, y respecto a los alcances de la Ciberdefensa, no existe diferencia alguna con los países de la OTAN considerando que tendrán responsabilidades nacionales,

[30] Traducción realizada por el autor.

internacionales y coaligadas con su aliados, esto queda plasmado en la Estrategia Nacional de Ciber 2022, donde el *Pilar N.º5* establece:

> Detectar, interrumpir y disuadir a nuestros adversarios mejorar la seguridad del Reino Unido en el ciberespacio y a través de él… para mejorar la seguridad del Reino Unido y de sus aliados, para mantener la seguridad del país y proteger y promover los intereses del Reino Unido dentro y fuera del país[31]. (Reino Unido, 2022. p:13)

3.4 Resultados del Capítulo

En el presente punto se exponen los resultados obtenidos luego de la comparación de las características estructurales de la Ciberdefensa en los países seleccionados como referencia. Para facilitar la recolección de los datos se ha estructurado un cuadro resumen, donde se describen los parámetros definidos para la comparación, los cuales fueron definidos en la metodología capitular como sigue: 1) Definición, 2) Propósito que busca, 3) Responsable y/o encuadramiento en el Estado, 4) Marco legal o regulatorio, 5) Principios o componentes que la rigen, y 6) Alcance (Fuerzas Armadas o Interagencial).

Tabla 2 Comparación de Características de la Ciberdefensa

	Definición	*Corresponde al conjunto de políticas y técnicas de la Defensa Nacional destinadas a enfrentar los riesgos y amenazas propias del ciberespacio de acuerdo con sus atribuciones constitucionales y legales. En lo específico, la CDef es una actividad del ámbito de la Defensa Nacional, que apoya a las operaciones militares y enfrenta las acciones hostiles en el CE, ejecutadas con fines militares o de inteligencia por parte de otros estados o por organizaciones ilícitas. La CDef se materializa mediante Ciberoperaciones (COps) que componen el empleo militar del CE. Las COps, a diferencia de las Operaciones Cinéticas, involucran principal, pero no exclusivamente, acciones en el CE.*
	Propósito	Proteger el ciberespacio en el ámbito de la Defensa Nacional y estratégico-militar.
	Encuadramiento	Ministerio de Defensa Nacional; Estado Mayor Conjunto, Dirección de Inteligencia de la Defensa.

[31] *Ídem*.

	Marco Legal o Regulatorio	Constitución Política de la República 1980. Art. N.º101; Política de Defensa Nacional 2020 y Ley Nº19.974.
	Principios	1) Inteligencia; 2) tecnología y; 3) cooperación
	Alcance (FAs o Interagencial)	Fuerzas Armadas e Interagencial, aun cuando la relación no queda definida solo sustentada en el principio de cooperación.
	Definición	*"acciones que lleva a cabo el Estado para proteger y controlar los posibles riesgos cibernéticos, con el objetivo de poder hacer uso del ciberespacio con tranquilidad, protegiendo de igual manera la integridad del territorio. La ejecución de la Ciberdefensa está al mando de las Fuerzas Armadas, quienes protegen las infraestructuras críticas del Estado…"*
	Propósito	En el contexto de la Defensa, centrarse en la fase operativa de contención de ciberataques, desarrollar defensa y protección de redes, información e infraestructura.
	Encuadramiento	Ministerio de Defensa; Comando General de las Fuerzas Armadas y Conjunto Cibernético.
	Marco Legal o Regulatorio	Constitución Política de Colombia (Respecto al rol de las Fuerzas Armadas en la Defesa Nacional"; CONPES 3701 - Lineamientos De Política Para Ciberseguridad y Ciberdefensa y CONPES 3854 - Política Nacional De Seguridad Digital.
	Principios o componentes	1) Personas; 2) Procesos; 3) Tecnología; 4) Cooperación; 5) Operaciones y; 6) Marco Legal.
	Alcance (FAs o Interagencial)	Fuerzas Armadas e Interagencial.
	Definición	*Conjunto de capacidades de defensa, explotación y ataque que permiten llevar a cabo operaciones en el ciberespacio, con la finalidad de preservar o ganar la libertad de acción en el ciberespacio de interés militar, impedir o dificultar su uso por parte del adversario, y contribuir a alcanzar la superioridad en el enfrentamiento en el resto de los ámbitos físicos y cognitivo.*
	Propósito	Preservar o ganar la libertad de acción en el ciberespacio de interés militar, impedir o dificultar su uso por parte del adversario, y contribuir a alcanzar la superioridad en el enfrentamiento en el resto de los ámbitos físicos y cognitivo.
	Encuadramiento	Ministerio de Defensa Nacional; Estado Mayor de la Defensa; Comando Conjunto del Ciberespacio.
	Marco Legal o Regulatorio	Constitución Española, Estrategia Nacional de Seguridad, Política de Seguridad Nacional, Política Nacional de Ciberseguridad, Manual Internacional de Tallin.
	Principios	1) Terminología Común; 2) Capacidades de Ciberdefensa; 3) Operaciones en el ciberespacio; 4) Integración a operaciones conjuntas; 5) Marco Legal; 6) Estructura de mando y control; 7) Integración Interagencial e Internacional; 8) Capacitación e Idoneidad del Personal e; 9) Inversión y desarrollo.
	Alcance (FAs o Interagencial)	Nacional, Interagencial, Internacional, coaligada.

	Definición	*Las acciones de defensa del ciberespacio se llevan a cabo dentro del ciberespacio protegido para derrotar amenazas específicas que han violado o amenazan con violar las medidas de seguridad del ciberespacio e incluyen acciones para detectar, caracterizar, contrarrestar y mitigar las amenazas, incluyendo el malware o las actividades no autorizadas de los usuarios, y para restaurar el sistema a una configuración segura.*
	Propósito	Alcanzar los objetivos de la nación en o a través del ciberespacio.
	Encuadramiento	Departamento de Defensa, Ciber Comando (Comando Combatiente Funcional).
	Marco Legal o Regulatorio	Estrategia de Seguridad Nacional, Estrategia Nacional de Ciber (2018), Estrategia del Departamento de Defensa para operar en el Ciberespacio (2018)
	Principios	Principios del Empleo Conjunto: 1) Simplicidad, 2) Agilidad y; 3) Economía de Fuerzas.
	Alcance (FAs o Interagencial)	Nacional, Interagencial, Internacional y Coaligada.
	Definición	acciones defensivas en o a través del ciberespacio para preservar la libertad de acción amiga en el ciberespacio
	Propósito	preservar la libertad de acción amiga en el ciberespacio y/o crear efectos para lograr los objetivos de los comandantes.
	Encuadramiento	Ministerio de Defensa, Comando Estratégico
	Marco Legal o Regulatorio	Ley de Servicios de Inteligencia de 1994 y la Ley de Poderes de Investigación de 2016, el DICA y el DIH, Manual Internacional de Tallin.
	Principios	1) Seguridad; 2) Sorpresa; 3) Concentración de Fuerza; 4) Mantención de la moral y; 5) Libertad de acción.
	Alcance (FAs o Interagencial)	Nacional, Interagencial, Internacional y Coaligada.

Nota: Tabla elaborada por el autor.

3.5 Validación de los resultados

Conforme a la experiencia de los especialistas, y principalmente a la luz de dos interrogantes: 1) La pertinencia del encuadramiento de la *Ciberdefensa* en la Dirección de Inteligencia de la Defensa (EMCO), y 2) Las características estructurales de la Ciberdefensa son suficientes para ser consideradas como un problema estratégico-militar. Se pudo hacer la triangulación necesaria para concluir respecto a cuáles son las características de la *Ciberdefensa* y además visualizar el marco general de países referentes en aspectos doctrinarios, así como en su desarrollo y evolución en *Ciberdefensa.*

Tabla 3 Opiniones de expertos: la ciberdenfensa como un problema estratégico.

Objeto de la pregunta	Especialista	Información obtenida
Pertinencia del encuadramiento de la Ciberdefensa en la DID	GDD. GRIFFITHS	"…no es pertinente, a mi juicio pasa por una parte debido a la ignorancia respecto a entender una nueva dimensión, por lo que se encuadra en algo conocido… pero no es algo de inteligencia…. luego a la coyuntura legal nacional, por el amparo de la Ley de Inteligencia" (11:00)
	GDD. PINO	El encuadramiento de la ciber en la DID es para darle un "paraguas" bajo el amparo de la Ley de Inteligencia. Tiene un sustento para poder realizar operaciones de las características que realiza. Le da una legitimidad no ilimitada (35:32)
	GDD. VARELA	Tiene que ver por una situación coyuntural política por la estructura nacional. La creación de un CC no es tan urgente como la gobernanza respecto a responsabilidades y definición de IC. (11:30). Gracias a la protección de la Ley de Inteligencia, se le enmarca ahí para estar al amparo. (12:44) Opino que es tan relevante la ciber que debiera ser independiente.
	GDB. GREZ	Creo que para dar respuesta al requerimiento de la Política Nacional de Ciberdefensa el año 2018 fue pertinente, ya que permitió trabajar al amparo de la Ley de Inteligencia, refuerzo que estoy de acuerdo con el momento que se vivía y estar bajo la ley permitía hacer operaciones intrusivas y contar con financiamiento para el desarrollo de capacidades. … sus alcances exceden a la amplitud de las operaciones de inteligencia y tiene concordancia con la necesidad de crear un Comando Conjunto, que reúna las capacidades para la coordinación de ciber operaciones y ciber inteligencia…
	CRL. VERA	Creo que era necesario en un principio, y fue consecuencia de otras cosas debido a que la asociaron como a capacidades de Guerra Electrónica, de ahí deriva el traspaso de la EW a inteligencia para quedar al amparo de la ley y en consecuencia la Ciberdefensa quedó ahí…. con los antecedentes y evolución abiertamente debe ser independiente de la inteligencia, pero siempre en el EMCO.
	CRL MELENDEZ	Obedece principalmente por el amparo de la Ley de Inteligencia, esto debido a que todas las acciones de intrusión … por tanto la única opción fue encuadrarlo acá e incluso hoy en día se ha dejado al DID como el futuro comandante de Ciberoperaciones, a mi juicio un error, pero así está concebido.
	CF SIÑA	A la luz de lo que vivimos hoy no es pertinente ya que sabemos que la función es mucho más allá de la exploración y solo la asesoría para la toma de decisiones, … eso sumado a las facultades de la Ley de Inteligencia. Lo importante hoy, no creo que sea que esté en

Objeto de la pregunta	Especialista	Información obtenida
		la DID, si es importante que esté en el EMCO y progresando en este nivel.
	TCL. VILLARROEL	El EMCO se encuentra en el proceso de estudio para la creación del Comando Conjunto de Ciberdefensa en un horizonte de mediano plazo. No obstante, … se estableció que depende de la Inteligencia Militar, ya que, en sus empleos, mantiene 3 roles fundamentales; - Defensivo (desde la seguridad informática a la tarea que realizan los CSIRTs). - Inteligencia (una capacidad de obtención de información). - Ofensivo (como capacidad que se mantiene asociada a una OEI). En este ámbito, cobran relevancia dos aspectos. En primer término, la relación de un organismo de carácter "directivo" como la DID, puede tener pertinencia sobre la Seguridad de Sistemas Informáticos y algún requerimiento de Inteligencia que pueda solicitarse a las Instituciones.
	SR. DIAZ DE V.	Fue por un tema de conocimiento y comprensión de tecnologías de información avanzada (15:50) cuando se crea la estructura de Ciberdefensa, las direcciones de inteligencia fueron las más avanzadas en esas materias y se podía construir desde una base. Creo que lo de la DID es irrelevante, *lo importante es que se haya generado en el EMCO como el gran coordinador y conductor estratégico, esa es la mirada que debemos dar.*
Las características de la Ciberdefensa son suficientes para ser consideradas como un problema estratégico-militar	GDD. GRIFFITHS	Absolutamente, es una dimensión que debe ser y será explotada por las componentes militares con las capacidades instaladas en busca del objetivo político entregado.
	GDD. PINO	Si son suficientes, especialmente por los impactos que tienen o pueden tener sus acciones (36:32). Además, por la capacidad de afectar a otros actores y otros intereses que comprometan aún más una opción de respuesta militar (41:04).
	GDD VARELA	Es un problema político estratégico, del más alto nivel (13:00), debido a los impactos y efectos en otros elementos del poder nacional.
	GDB. GREZ	Claro que sí, las capacidades de afectar tanto el ambiente de la información, como acciones físicas deben ser consideradas estratégicas especialmente basado en los efectos que estas acciones tienen. Abiertamente la Ciberdefensa puede afectar la toma de decisiones al más alto nivel al punto de disuadir o deslegitimar una postura contrapuesta a los intereses propios.
	CRL. VERA	De todas maneras, creo incluso que aún no dimensionamos los efectos que se pueden causar en forma encubierta, quién domine este ámbito puede definir el conflicto sin disparar un tiro.
	CRL. MELENDEZ	Creo que con todo lo que hemos hablado, puedo decir que a pesar de que el deber ser no se cumple, por definición o por concepción si lo es.

Objeto de la pregunta	Especialista	Información obtenida
	CF SIÑA	Creo que desde muy temprano se entendió esto desde las instituciones, hasta que se asume que debe ser planificado y coordinadas en el nivel estratégico.
	TCL. VILLARROEL	Porque proviene desde la Política de Ciberseguridad, que persigue alcanzar una condición de Seguridad en el Ciberespacio… por lo que la Ciberdefensa representa el aporte del sector Defensa para tal objeto…en este sentido, este es un problema del nivel estratégico de la conducción militar.
	CRL. BURBANO	Enfrentar los problemas y retos de conexión a las tecnologías de la información y las comunicaciones está determinada por estos dos términos (Ciberdefensa y Ciberseguridad) con los cuales se han planteado alternativas metodológicas, políticas, normas y procedimientos. De esta manera se define la Ciberdefensa como la capacidad del Estado para prevenir y contrarrestar toda la amenaza o incidente de naturaleza cibernética que afecte la **soberanía nacional**, por lo tanto, es del más alto nivel.
	SR. DIAZ DE V.	Respecto a todo lo conversado con anterioridad y la necesidad de mantener la Ciberdefensa en el EMCO, es el mejor indicador que el entorno de la Ciberdefensa es un problema militar estratégico.

Nota: Tabla elaborada por el autor.

A la luz de los resultados de la exploración doctrinaria, que dio el marco de comprensión acerca de cuáles son las características estructurales de la *Ciberdefensa*, es posible concluir en términos generales, que las definiciones vienen a hacer referencia de la acción de mitigar *riesgos y amenazas*, que pueden afectar la *Seguridad Nacional* o los *Intereses Nacionales.* Por otro lado, se identifica en la mayoría de ellas que el propósito es generar el libre uso del ciberespacio, utilizándose de sobremanera el término de *libertad de acción* propios y de los países amigos o aliados.

Las consideraciones del encuadramiento o mandos responsables queda claramente establecido que: primero todos se encuentran en el *Sector Defensa*; segundo independiente si es un *Comando Conjunto*, un *Departamento* o *Dirección*, una unidad *Directiva* o *Ejecutiva*, todos sin distinción están inmediatamente bajo los Ministerios de Defensa, y por sobre las *Instituciones, Servicios* o *Ramas* (Ejército, Armada o Fuerza

Aérea) adquiriendo una connotación *Conjunta*, es decir, dependiente directo del *Nivel Estratégico.*

Respecto a la presencia del marco regulatorio, es posible identificar que todos los países estudiados, abiertamente asimilan la normativa nacional particular y aquella del Derecho Internacional o de los Conflictos Armados. Se puede inferir de lo anterior que todos los países estudiados asumen su rol como *Sujeto del Derecho Internacional,* ya que aquellos que no explicitan las responsabilidades en el extranjero, si adhieren al marco constitucional vigente, por lo que se obligan a lo mandatado por los tratados internacionales, y a la ley interna de cada uno de ellos.

Otro punto abordado fue la definición de principios fundamentales o estructurales de la *Ciberdefensa*, donde fue posible identificar dos tipos; el grupo de países que la entienden como el sistema completo (políticas, capacidades y acciones) donde los principios son abiertamente orientados al desarrollo permanente de capacidades, así como integración y coordinación respectivamente. El otro grupo, que define la *Ciberdefensa* como una parte de las *ciberoperaciones* asume un rol de acción conjunta, determinando la necesidad de la comprensión y respeto de los *principios de la acción conjunta*, ciertamente vinculados con algunos de los *principios de la guerra* de cada doctrina.

El último punto de la indagación doctrinaria fue la determinación de los alcances con los cuales se concibe la *Ciberdefensa* (Interagencial, internacional, etc.). El resultado fue evidente, tácito o no, con designación de responsabilidades y/o desarrollo de organismos ya establecidos para vincularse, por tanto ha sido posible concluir que la *Ciberdefensa* es a lo menos Interagencial, para algunos internacional y coaligada, lo que ha permitido concluir que sus alcances están por sobre el *Sector Defensa*, es decir, tienen implicancias con otros actores de la política nacional o internacional según corresponda.

Las intervenciones de los especialistas, específicamente para el caso de Chile permiten establecer a pesar de encontrarse la *Ciberdefensa* bajo una *Dirección* del EMCO, que lo relevante obedece, primero a que fue una decisión coyuntural de la época; segundo que donde se enmarcó tiene una protección y delimitación legal (tanto de acción como de presupuestos), independiente si hoy es el encuadramiento ideal y;

tercero y más importante rescatando las palabras de Gonzalo Diaz de Valdés *"lo importante es que se haya generado en el EMCO como el gran coordinador y conductor estratégico, esa es la mirada que debemos dar".*

Por último, independiente de la mirada técnica en el sentido de la acción, o estratégica en la concepción macro de la Ciberdefensa, tanto en las doctrinas analizadas como en las opiniones vertidas hay un consenso que las características estructurales de la Ciberdefensa la posicionan en el ámbito de lo *estratégico-militar* e incluso en lo *político-estratégico*, según la mirada de algunos de los especialistas.

3.6 Síntesis del capítulo

El propósito del capítulo fue determinar cuáles eran la características estructurales de la *Ciberdefensa*, donde la metodología involucró la indagación en las doctrinas referentes seleccionadas y publicaciones afines como por ejemplo aquellas de la OTAN. Para el análisis se seleccionaron seis aspectos considerados como comunes en las estructuras, los cuales fueron definidos como: 1) Definición, 2) Propósito que busca, 3) Responsable y/o encuadramiento en el Estado, 4) Marco legal o regulatorio, 5) Principios o componentes que la rigen, y 6) Alcance (Fuerzas Armadas o Interagencial). Los resultados obtenidos fueron una serie de consideraciones técnicas y conceptuales donde se pudo destacar que, primero todos se encuentran en el *Sector Defensa,* segundo todos cuentan con un marco regulatorio, tercero obedecen a principios de desarrollo o empleo claramente definidos según las realidades particulares y; por último, todos tienen incidencia al menos Interagencial.

En un segundo momento se tomó en consideración la opinión de los especialistas nacionales, además de un integrante del Ejército Nacional de Colombia, para abordar los temas tratados y confrontarlos con su experiencia, específicamente en dos ámbitos; la pertinencia del encuadramiento de la *Ciberdefensa* en la DID y, por otro lado, y a la luz de los antecedentes presentados, si era pertinente o no considerarla como un asunto del nivel estratégico-militar.

Finalmente, los resultados del capítulo se expresan en términos de conclusiones del autor respecto a las realidades doctrinarias investigadas y la experiencia de los

especialistas, cumpliendo con creces la identificación de las características estructurales, objetivo del capítulo, y pudiendo ya proyectar como estas se van asociando al nivel de la conducción estratégica nacional.

CAPÍTULO IV
LAS VARIABLES OPERACIONALES Y LOS PRINCIPIOS DE LA GUERRA CONJUNTOS

4.1 Metodología del capítulo

El presente y último capítulo de la investigación, tuvo por objetivo dar respuesta a las dos interrogantes que se han planteado respecto a los factores de análisis de la Ciberdefensa en el contexto nacional, donde los seleccionados fueron las *variables de análisis estratégicas nacionales* (PEMSII-PT) y *los principios de la guerra conjuntos.* Respecto de las primeras se han seleccionado las siguientes: 1) militares, 2) infraestructura e, 3) información como una manera de acotar la indagación, indistintamente que puedan afectar a las otras. Desde el punto de vista de los *principios de la guerra* se seleccionaron todos los considerados en DNC – 0 *"Doctrina para la Acción Conjunta de las Fuerzas Armadas"* los cuales son: 1) Objetivo, 2) Ofensiva, 3) Concentración, 4) Economía de Fuerzas, 5) Maniobra, 6) Unidad de Mando, 7) Seguridad, 8) Sorpresa y, 9) Simplicidad.

A diferencia de los capítulos anteriores que, a través de un estudio comparado de las doctrinas y documentos de investigación, fue factible identificar qué es y cómo se entiende un *problema estratégico* y, por otro lado, cuáles son las *características estructurales* de la Ciberdefensa, en este capítulo el foco estuvo en la Doctrina Nacional Conjunta y cómo se puede y debe vincular la Ciberdefensa a las decisiones del nivel estratégico considerando los factores seleccionados, indicados en el párrafo anterior.

Independiente de lo anterior, se utilizaron como aporte al análisis, antecedentes de los países referentes y publicaciones académicas no con el fin de comparar, sino con el propósito de ampliar la comprensión y amplitud de los elementos que influyen en esas doctrinas o bien en el campo de batalla moderno, donde la Ciberdefensa ya ha jugado roles protagónicos desde el punto de vista de la configuración del ambiente de la información, o bien como maniobra de configuración desde el ciberespacio hacia los otros dominios de la guerra. Lo anterior permitió concluir cuáles son los antecedentes

que se deben considerar al momento de emplear la Ciberdefensa en la planificación de una opción de respuesta militar (ORM).

Por último, se buscó a través de las entrevistas a especialistas, corroborar lo establecido en la doctrina, así como obtener opiniones actualizadas respecto a su experiencia, lo que permitió la saturación de algunos conceptos dando sustento y rigurosidad científica a los hallazgos del capítulo, pudiendo finalmente concluir, acerca de la identificación de las *variables de análisis estratégicas* (PEMSII-PT) y los *principios de la guerra conjuntos.*

4.2 Las variables de análisis estratégicas

Antes de adentrarse en la descripción de las variables seleccionadas, se estimó pertinente establecer el por qué las PEMSII-PT fueron las seleccionadas o calificadas, para la presente investigación, como *variables de análisis estratégicas.* Es preciso señalar que tras haber determinado el significado de *problema militar* y cuáles son los alcances del *nivel de la conducción estratégico* a nivel nacional, es congruente establecer, que las variables de análisis deben estar alineadas con lo que establece la doctrina nacional, por cuanto la metodología PEMSII-PT es la adecuada. Durante la exploración no se menciona en ninguna de las fuentes consultadas, cómo desarrollar la metodología de análisis, ni tampoco por qué fue seleccionada para la planificación conjunta, pero si se hace referencia a ella en los procesos de planificación.

Ejemplo de lo anterior es que en el texto matriz de la doctrina nacional, DNC-0 *"Doctrina para la Acción Conjunta de las Fuerzas Armadas"*, no nombra a estas variables de análisis, solamente hace presente que en el nivel estratégico se debe planificar el empleo de los medios conjuntos en un *marco operacional* en el que *"se está inserto en un sistema en el que los efectos de las acciones militares, interaccionan con las de otros elementos: políticos, económicos, diplomáticos, legales, sociales, entre otros"* (Ministerio de Defensa, 2011. p:31). De lo anterior, se pudo identificar que existen algunas variables que afectan directamente las operaciones militares, donde si bien no se listan las PEMSII-PT, al menos considera algunas de ellas y más importante aún, establece el concepto de interrelación entre el ámbito militar y las variables señaladas.

Es destacable señalar que la DNC- 5-0 *"Doctrina Conjunta para la Planificación de Operaciones de las Fuerzas Armadas"*, ya hace uso de estas variables de análisis en diferentes momentos de la planificación, donde por ejemplo, son nombradas en la *Etapa II "Orientación"* exponiendo que durante la *Revisión de la Situación* se deben tener en consideración los antecedentes estratégicos que incluyen *"la influencia que los factores históricos, políticos, militares, económicos y sociales puedan tener en las operaciones. También se deben considerar las implicaciones del derecho humanitario y de las leyes internacionales"* (Ministerio de Defensa, 2011. p:46).

En adición a lo anterior, en la etapa de *Desarrollo del Concepto*, específicamente en el punto denominado *Factores de Tiempo o Circunstancias* señala que:

> Se refiere a los tiempos en todas sus implicancias, condicionantes impuestas por la situación que se vive o vivirá, causas del estado indeseado que genera la operación o campaña, riesgos, estatus jurídico, presunciones, restricciones e imposiciones externas, situación de toda índole política, estratégica, social, económica, etc. (Ministerio de Defensa, 2011. p:53)

Luego, en el acápite de *Factores de Espacio o Lugar* se señala que constituye:

> …el escenario dentro del cual se cumplirá la misión, referidos al teatro o área de operaciones, con sus dimensiones terrestre, marítima, aérea, espacial, ciberespacio y espectro electromagnético que conforman el espacio de batalla, factores fijos o variables propios del lugar…también importan las instalaciones militares, sociales y económicas, el medio ambiente y los espacios protegidos, condiciones sanitarias, las vías de comunicaciones y sus terminales terrestres, marítimos y aéreos, las comunicaciones, ciencia y tecnología y todo tipo de recursos existentes y disponibles. (Ministerio de Defensa, 2011. p:53)

La misma publicación doctrinaria, en su apartado dedicado a la planificación de *Inteligencia*, específicamente en la etapa de *Orientación,* establece que *"Participa activamente entregando antecedentes… en particular aquellos referidos al ambiente operacional desde la perspectiva de las diferentes dimensiones (terrestre, marítima,*

aérea y del espacio) y de los factores políticos, económicos, militares, sociales, de infraestructura e información (PEMSII)" (Ministerio de Defensa, 2011. p:75). Por último, este reglamento posee dos anexos donde se sugieren: 1) La agenda para la Reunión de Análisis de la Misión, y 2) Guía de Planificación del Comandante (GPC). En el primer documento se sugiere que se incluyan antecedentes debido a que: *"las influencias de los factores históricos, políticos, militares, económicos y sociales en la situación y su potencial influencia en las operaciones a realizar. También debe considerarse el impacto del Derecho Internacional y Humanitario conforme al nivel de planificación"* (Ministerio de Defensa, 2011. p:91).

En el segundo texto, al igual que el anterior establece que en los antecedentes generales para iniciar la GPC se deben considerar al menos aquellos que aporten antecedentes *"Históricos, políticos, económicos, sociales y militares"* (Ministerio de Defensa, 2011. p:96).

Otro reglamento conjunto que establece estas variables es la DNC 2-4 *"Preparación de Inteligencia del Ambiente Operacional Conjunto (JIPOE)",* donde desde su *Capítulo I* establece claramente que *"El JIPOE se emplea para efectuar un análisis del ambiente físico (aire, tierra, mar y espacio) de información (que incluye el ciberespacio), los sistemas políticos, militares, económicos, sociales, informaciones e infraestructura (PMESII)"* (Ministerio de Defensa, 2013. p:8). Lo planteado en este párrafo, a juicio del autor, adquiere el valor y sustento necesario para reafirmar que, se debe considerar el comportamiento de la Ciberdefensa basado en las variables señaladas considerando que; primero, el concepto enmarca que se deben analizar los dominios, aire, tierra, mar y espacio, incluyendo al ciberespacio y; segundo que el análisis debe ser en base a los factores PEMSII-PT o PMESII como los trata el reglamento señalado.

Además de lo anterior, otro aspecto a considerar desde el punto de vista doctrinario, es que el mismo manual establece que la importancia de utilizar esta metodología de análisis es que permitirá:

> …visualizar y describir cómo interactúan los factores políticos, militares, económicos, sociales infraestructura e informaciones, para facilitar el empleo de la fuerza y la cooperación con sus contrapartes u otros organismos

intergubernamentales y/o interagenciales, que puedan estar fuera del ámbito del JC[32] (Ministerio de Defensa, 2013. p:63).

Habiendo comprobado que las variables PEMSII-PT son aquellas impulsadas por la doctrina nacional para el análisis de la planificación conjunta, tanto en el nivel estratégico como operacional, además de corroborar que se incluye en dicho análisis el 5to dominio de la guerra, quedó establecido el contexto para identificar cuáles son las implicancias que se deben tener en consideración para la planificación considerando la Ciberdefensa, particularmente en las variables *militares, infraestructura e informaciones.*

Como fue expresado al inicio del capítulo, las variables PEMSII-PT fueron las seleccionadas por el autor para identificar el comportamiento de la Ciberdefensa en ese contexto, aun cuando no se explica en la doctrina conjunta el motivo de su elección como metodología, solo se puede inferir, que por su amplitud abarca una mirada global del ambiente operacional. Por otro lado, tampoco se describen como deben ser utilizadas cada una de las variables o la delimitación de su uso, por lo que fue necesario acudir a la doctrina base de los Estados Unidos, en específico el homólogo de la DNC 2-4, el reglamento JP 2-01-3 *"Joint Intelligence Preparation of the Operational Environment".* Este documento, en el acápite de desarrollo de la perspectiva de sistemas, dedica algunas páginas al desarrollo de cada una de las variables donde se puede destacar lo reflejado en la Tabla N.º2, conforme a la delimitación impuesta.

Con los antecedentes expuestos en la tabla, fue posible acotar el escenario para poder identificar cuál es el comportamiento y las consideraciones con las que influye la Ciberdefensa en cada una de las variables, y qué se deben tener a la vista en la planificación de las operaciones militares en el nivel estratégico. Lo que no se puede obviar en el análisis son los siguientes aspectos; primero, considerar las características del ciberespacio; segundo, que la experiencia fue tomada de otros países y; tercero, el espíritu es netamente doctrinario y generalista, por lo que no obedece al análisis profundo de una operación en particular.

[32] JC, hace referencia al Comandante Conjunto por sus siglas en inglés *Joint Commander.*

Tabla 4 Resumen de las Variables PEMSII-PT[33]

Militar	Las consideraciones militares pueden incluir, entre otras, las siguientes: ROE[34]; establecimiento y ubicación de zonas de exclusión marítimas y zonas de exclusión aérea; zonas de defensa marítima; aguas territoriales; reclamaciones marítimas excesivas; y zonas de identificación de defensa aérea. Sin embargo, hay que tener cuidado al analizar el impacto de las limitaciones militares que no imponen restricciones físicas reales (como los obstáculos creados por el hombre) y que, por tanto, podrían ser muy transitorias. (Estados Unidos, 2014. p:92)
Informaciones	Las consideraciones deben centrarse en las fuentes y medios a través de los cuales la información llega a la población general en el área de interés. Éstas pueden incluir fuentes oficiales, como los medios de comunicación controlados por el gobierno; fuentes no oficiales, como los medios de comunicación locales independientes; fuentes internas no autorizadas, como la radio y los periódicos clandestinos; y fuentes de terceros, como la prensa internacional y diversos medios de comunicación social. Los analistas también deben centrarse en los medios por los que la información se difunde y se comparte dentro de la estructura de liderazgo del adversario. La credibilidad de los distintos medios y fuentes de información, tal y como la perciben los grupos implicados, es fundamental. (Estados Unidos, 2014. p:93)
Infraestructura	Las consideraciones pueden incluir, entre otras, las fuentes de agua potable; los medios y sistemas de transporte (redes de carreteras y ferrocarriles, canales y vías fluviales); los nodos de comunicaciones; las instalaciones de producción de energía y las redes de transmisión; las tuberías; y las instalaciones de tratamiento médico. Es importante evaluar no sólo el estado actual de la infraestructura del adversario, sino también el impacto de las operaciones militares proyectadas en la infraestructura que puede ser crítica para la recuperación después del combate. (Estados Unidos, 2014. p:93)

Nota: Tabla elaborada por el autor.

Durante la indagación fue evidenciado que, en documentos de estudios y publicaciones doctrinarias, se hace recurrente encontrar el uso de la metodología PEMSII-PT, no obstante, no se entregan detalles de la manera de cómo utilizarlos, o experiencias de sus conclusiones como ya fue indicado en párrafos anteriores. Los puntos en la doctrina nacional ya fueron nombrados, así como una descripción acotada de la doctrina de los Estados Unidos.

En otro orden de ideas, ha sido pertinente nombrar una publicación reciente de la OTAN, acerca de la mejora del proceso de toma de decisiones en sistemas complejos. Desde el punto de vista del nivel de la conducción se estima adecuado, ya que el

[33] Traducción de las definiciones de las variables seleccionadas fueron hechas por el autor.
[34] ROE, sigla en inglés para *Rules of Engagement.* Reglas de Enfrentamiento.

enfoque está en: *"comprender el ambiente operacional; definir el problema; visualizar el estado final deseado militar; e intervenir con un enfoque operativo óptimo (modos/medios) para lograr el estado final deseado militar"*[35]*.* (Angellini, Maymir-Ducharme & Stapleton, 2021. p:1), es decir, no involucra el nivel político-estratégico o gran estrategia. Por otro lado, hace referencia en el cómo modelar escenarios de guerra híbrida y la importancia de desarrollar las capacidades de entender *"aspectos humanos del entorno operacional a través de estas variables del entorno operacional: políticas, militares, económicas, sociales, de información, de infraestructura, del entorno físico y del tiempo (conocidas como PMESII-PT)"* [36] (Angellini, Maymir-Ducharme & Stapleton, 2021. p:3).

A lo anterior, podemos agregar que, en atención a lo contemporáneo del estudio, se menciona la dimensión del ciberespacio y sus características; *"Las tecnologías cognitivas y de sistemas sociales cibernéticos se aplicarán para ayudar a los responsables de la toma de decisiones a comprender las relaciones "causales circulares" y las interacciones de las variables del PMESII-PT que influyen y desencadenan el cambio en el EO"* [37]*.* (Angellini, Maymir-Ducharme & Stapleton, 2021. p:4). Por último, el mismo texto finaliza aseverando que:

> …para ganar en un entorno complejo y persistente, los responsables de la toma de decisiones pueden aplicar conceptos de dinámica de sistemas …para capturar el entorno físico, los factores cognitivos, organizativos, sociales y culturales de las variables del PMESII en el espacio y el tiempo que son críticos en el espacio de batalla urbano [38]. (Angellini, Maymir-Ducharme & Stapleton, 2021. p:20)

Todo lo anterior, permite identificar que estas variables están totalmente vigentes para el análisis de ambientes operacionales que involucran el ciberespacio, y condiciones complejas de estructuración de los escenarios. Sin embargo, nuevamente se ponen los énfasis, en considerar las variables debido a su amplitud, pero no se evidencia cómo o cuál es el comportamiento concreto de ellas. No obstante, un hallazgo importante para la presente investigación, fueron los resultados del ejercicio de

[35] Traducción realizada por el autor.
[36] *Ídem.*
[37] *Ídem.*
[38] *Ídem.*

simulación realizado por el *Interservice/Industry Training, Simnulation, and Education Conference (II/ITSEC)* del año 2016, este ejercicio fue denominado "*Simulation of Cyber Impacts on PMESII-PT Variables"*[39]*,* y es aquí donde se pudieron evidenciar resultados concretos en el comportamiento de las variables seleccionadas.

El propósito del ejercicio señalado era, a través de dos sistemas de simulación, demostrar como *"los factores financieros, sociales y gubernamentales pueden verse afectados por las operaciones cibernéticas disruptivas, de tal manera que impidan las operaciones militares"*[40] (Cerri, Sleevi, 2016. p:2)*.* En el acápite que hace referencia a la creciente importancia de las operaciones de ciber en el ambiente operacional, hace una breve descripción de las características del ciberespacio donde se destaca, además de lo ya establecido en esta investigación, que resaltan algunos atributos como: 1) Dominio creado por el hombre, 2) Ambiente, tácticas, técnicas y procedimientos que involucran gran velocidad, 3) Presencia constante en todas las fases de la operación, y 4) ilimitado e instantáneo.

Específicamente en aquello de interés para la investigación, el estudio inició con una fase descriptiva de las variables PEMSII-PT, lo que arrojó como diagnóstico de la influencia de Ciberdefensa en las variables seleccionadas lo siguiente:

Tabla 5 Posible impacto en variables y subvariables PEMSII-PT

Militar	Información	Infraestructura
- Fuerzas Militares. - Fuerzas paramilitares de Gobierno. - Fuerzas paramilitares no gubernamentales. - Combatientes armados no militares. - Funciones de Combate.	- Medios de Comunicación. Pública. - Guerra de Información - Inteligencia. - Administración de la información.	- Patrones de Construcción. - Zonas urbanas. - Zonas urbanas en construcción.

Nota: Tabla elaborada por el autor a partir del cuadro. *"Descriptive Analytics Used for Characterizing the PMESII-PT Variables*" (Cerri; Sleevi, 2016).

Dentro de las consideraciones que fueron tomadas para seleccionar las variables anteriores, fue que se propone que el ambiente operacional puede incluir entre otros:

[39] "*Simulación de los impactos de Ciber sobre las variables PEMSII-PT".* Traducción realizada por el autor.
[40] Traducción realizada por el autor.

1) Aliados Estratégicos (OTAN, ONU, Banco Mundial, etc.), 2) Aliados Interagenciales, 3) Aliados Multinacionales y, 4) Organizaciones no gubernamentales (ONGs). Por otro lado, las ciberoperaciones de la fuerza enemiga consideró: 1) Denegación de Servicio Distribuida (DDoS), 2) Infección con virus, 3) Ciber sabotaje a infraestructura crítica, 4) Sistemas de la red eléctrica y, 5) Ataques a la red principal de internet.

La conjugación de los actores militares y civiles, así como los efectos de los ataques en todo espectro, tanto a las tropas como a la población local, trajeron los siguientes resultados específicos para cada una de las variables seleccionadas que, entre otros, son factibles de destacar:

Tabla 6 Resultado sobre las variables MII

Militar	Información	Infraestructura
- Desgaste de las tropas regulares en el desempeño de sus actividades de despliegue. - Intención y objetivos comprometidos por el factor tiempo. • Factor: Tropas *"Los ciberataques frenaron el ímpetu de las Fuerzas Azules y dieron tiempo a que se reforzaran las Fuerzas Rojas". (Cerri; Sleevi, 2016. p:8)*	- Medios y el contenido de los medios de comunicación. - Operaciones de Información e inteligencia. - Cooperación y HUMINT.[41] - Educación. • Factor: Percepción *"Los ciberataques afectaron a los sistemas comerciales y de gobierno… Esto incluía todos los medios de comunicación basados en Internet y la radio/televisión".* *"Los ciberataques se llevaron a cabo para permitir el uso del ciberespacio para difundir propaganda, atacar sitios web y robar dinero para financiar actividades o para planificar y coordinar delitos en el mundo físico" (Gandhi,*	- Propiedad privada. - Paquetes de activos de información. - Plantas de producción de servicios y bienes. • Factor: Propiedad fiscal y privada *"Los ciberataques afectaron a la composición de las instalaciones y servicios básicos necesarios para el funcionamiento eficaz de la comunidad o sociedad. Las poblaciones locales dependen… de un entorno de "Internet de las cosas" para todos los aspectos de los sistemas logísticos, junto con las redes civiles financieras y de infraestructura, de transporte, medios de comunicación, banca y actividad económica cotidiana. En la mayoría de los casos, las*

[41] HUMINT, de sus siglas en inglés *"Inteligencia Humana".*

	2012). en (Cerri; Sleevi, 2016. p:8)	*pérdidas físicas se producen cuando el mundo cibernético está estrechamente integrado con el mundo físico, como en el caso de los sistemas que controlan la distribución de energía, gas, agua, alcantarillado, petróleo y otros servicios críticos".* (Cerri; Sleevi, 2016. p:8)

Nota: Tabla y traducciones elaboradas por el autor.

Los resultados del ejercicio de simulación, ciertamente son mucho más amplios en el sentido de las otras variables de PEMSII-PT, así como en los aspectos técnicos de los sistemas de simulación empleados para el levantamiento del ambiente operacional. Los datos entregados por este estudio, así como los antecedentes de la doctrina nacional y extranjera, permiten obtener algunas conclusiones.

En primera instancia, y desde el punto de vista de la homologación del nivel de la conducción, tanto en la doctrina nacional como en la extranjera, ya sea Estados Unidos o aquella pertinente a la OTAN, utilizan las variables PEMSII-PT como marco de trabajo, análisis y planificación. Por lo tanto, se deduce; primero la Ciberdefensa está enmarcada dentro de un dominio de la guerra; segundo las variables seleccionadas están en el orden del análisis del *estado final deseado militar*, es decir, no sobrepasa lo político-estratégico o gran estrategia y; tercero los resultados de la simulación de ciberoperaciones en términos de sus efectos, permiten evidenciar que una acción militar (ciberataques) tuvo repercusiones directas en: 1) las tropas, 2) en el ambiente de la información local (militar y civil) y, 3) en la infraestructura atacada (civil y militar), por lo que se evidencia un problema del más alto nivel de la conducción, por su complejidad; alcance (inter agencialidad), comprometimiento de los objetivos militares y, en consecuencia del *estado final deseado militar*.

4.3 Los principios de la guerra conjuntos

El otro factor de análisis seleccionado para determinar el por qué la Ciberdefensa es un problema del nivel de la conducción estratégica, fueron los postulados teórico-

prácticos de *los Principios de la* Guerra, a través de la identificación de su aplicabilidad para la Ciberdefensa en este nivel de la conducción. Al igual que muchos otros conceptos estudiados en la investigación, no existe consenso académico de cuáles son, más bien, tras la exploración fue posible afirmar que cada autor (Sun Tzu, Clausewitz, Jomini, Fuller, etc.), Institución (Ejército, Armada o Fuerza Aérea) o nivel conjunto nacional o multinacional (Chile, Estados Unidos, OTAN), define los propios conforme a su experiencia y realidad.

En atención a lo planteado anteriormente, sin el afán de sobre teorizar el concepto, ya que no es el objeto de esta investigación, es pertinente establecer que se entiende por *Principios de la Guerra*, y declarar que la delimitación de la investigación se centra en la Doctrina Nacional Conjunta, para determinar su aplicación a través de la Ciberdefensa en el 5to dominio de la guerra. Dichos principios son: 1) Objetivo, 2) Ofensiva, 3) Concentración, 4) Economía de Fuerzas, 5) Maniobra, 6) Unidad de Mando, 7) Seguridad, 8) Sorpresa y, 9) Simplicidad.

Luego de la revisión bibliográfica tanto de la doctrina conjunta de Chile, como extranjera, así como la revisión y análisis de diferentes publicaciones militares afines, es posible ratificar lo expresado en el párrafo precedente con respecto a que la definición viene determinada por la necesidad de cada usuario de dichos principios. Un estudio comparado del Capitán de Corbeta Reinaldo Rivas González de la Armada de Chile, propone que una manera de definir el concepto es *"el carácter de ideas matrices sobre los principales aspectos de la guerra, que abarcan por lo general todos los niveles de actividades, desde la formulación de una gran estrategia al simple empleo de un buque menor"* (Rivas, 1968. p:01).

Por su parte, la Doctrina Nacional Conjunta, no propone una definición, pero antes de describirlos, plantea que es básico para cualquier doctrina el conocimiento de principios y normas que han regido, exitosamente, la guerra en conflictos del pasado, aun cuando no debe entenderse como máximas absolutas, ya que dependiendo de cada situación, cobrarán relevancia algunos principios más que otros, pero se destaca la importancia de su conocimiento por parte de los comandantes y planificadores para comprender y conducir las operaciones.

Por otro lado, el Mayor David Farmer de la Fuerza Aérea de los Estados Unidos, y como parte de sus estudios en la *Escuela de Estudios Militares Avanzados,* establece que *"Los principios de la guerra proveen una visión de nuestra comprensión a los fundamentos de las operaciones militares…son una guía para la eficacia… y los líderes de los Estados Unidos, los utilizan para asegurar la preparación de sus tropas"*[42] (Farmer, 2010).

Por último, se ha encontrado pertinente la visión que expone el Mayor General PK Mallik, quién en su artículo *"Principles of War, time for Re-Look"* hace mención abiertamente a lo siguiente:

> Nunca ha habido un acuerdo universal sobre una lista común de principios. La mayoría de las naciones tienen su propia lista de principios basada en su cultura militar, su experiencia y su patrimonio. Los Principios de la Guerra son una guía para las acciones relativas a la aplicación del poder de combate, más que una verdad incuestionable con aplicación universal a cada operación[43]. (Mallik, 2020)

Conjugando las visiones expuestas en los párrafos anteriores, fue posible determinar que estos principios, son una guía que concentra parámetros de empleo de fuerzas militares, identificados e individualizados en las guerras del pasado, que permiten a los comandantes de todos los niveles de la conducción, contar con una pauta flexible para la preparación de sus tropas, la planificación de sus operaciones militares y conducción de las mismas, sin ser una máxima inamovible, muy por el contrario, son flexibles a cada situación y cobrarán énfasis diferenciados conforme al ambiente operacional que se presente.

La Doctrina Nacional Conjunta ha establecido nueve *principios de la guerra* para este nivel, los cuales ya han sido nombrados en este capítulo. La investigación permitió comprobar que los nueve principios conjuntos son iguales a los que presenta la doctrina conjunta de los Estados Unidos, en el *JP 3-0 Joint Operations,* la diferencia es que este manual además considera tres principios nuevos, conforme han

[42] Traducción realizada por el autor.
[43] *Ídem.*

evolucionado las operaciones militares durante el último siglo. Estos principios son: 1) Restricción, 2) Perseverancia y, 3) Legitimidad, que según se explicita en el mencionado manual, le permite a los Estados Unidos operar en la amplia gama de operaciones militares. Todo lo anterior, se ha descrito para poder establecer que el uso de ejemplos asociados a ciberoperaciones de la doctrina estadounidense, es aplicable a la doctrina chilena, excepto en los tres principios diferenciados.

Cómo último punto, antes de demostrar la aplicabilidad de los principios de la guerra a través de la evidencia en la doctrina o publicaciones militares, se estima pertinente exponer un resumen de las definiciones de los nueve principios, destacando las diferencias con la doctrina de los Estados Unidos, con el único fin de facilitar la comprensión de ellos.

Tabla 7 Comparación de Principios de la Guerra Conjuntos Chile – Estados Unidos

Principio		 [44]
1. Objetivo	…dirigir cada operación militar hacia un resultado claramente definido, decisivo y accesible. El objetivo de las operaciones de combate es la destrucción de las capacidades de las Fuerzas Armadas del enemigo y de su voluntad de lucha.	(1) Dirigir cada operación militar hacia un resultado claramente definido, decisivo y accesible. (2) Alcanzar objetivos que contribuyan al objetivo estratégico… el Comandante Conjunto debe evitar acciones que no contribuyan directamente al objetivo superior. (3) El objetivo militar puede cambiar, si el objetivo nacional cambia y el Comandante Conjunto debe poder anticipar este cambio.
2. Ofensiva	…tomar, retener y explotar la iniciativa. La acción ofensiva es la forma más eficaz y decisiva de lograr un objetivo claramente definido. …son el medio por el cual una fuerza militar toma y retiene la iniciativa, … mantiene la libertad de acción y logra resultados decisivos.	(1) Tomar, retener y explotar la iniciativa. (2) La acción ofensiva es la forma más eficaz y decisiva de lograr un objetivo claramente definido. son el medio por el cual una fuerza militar toma y retiene la iniciativa, … mantiene la libertad de acción y logra resultados decisivos. Su importancia es en todos los niveles de la conducción.
3. Concentración (Mass)	…concentrar los efectos de la potencia de combate en un lugar	(1) …concentrar los efectos de la potencia de combate en un lugar y

[44] Traducciones realizadas por el autor.

	y a una hora que permitan que la fuerza logre resultados decisivos. La concentración siempre debe ser sostenida para tener el efecto deseado. La concentración de los efectos, más que la concentración de fuerzas puede permitir que fuerzas, aun numéricamente inferiores, logren resultados decisivos y minimicen las pérdidas humanas y el gasto de recursos.	momento que permitan que la fuerza logre resultados decisivos. (2) Para alcanzar la concentración, las capacidades de la fuerza conjunta son sincronizadas e integradas donde puedan generar efectos decisivos durante un corto tiempo. La concentración de los efectos, más que la concentración de fuerzas puede permitir que fuerzas, aun numéricamente inferiores, logren resultados decisivos y minimicen las pérdidas humanas y el gasto de recursos.
4. Economía de Fuerzas	…asignar la potencia de combate esencial mínima a los esfuerzos secundarios. Es el empleo y la distribución prudente de fuerzas con la finalidad de lograr concentración de medios en un determinado lugar o punto para el momento de la decisión.	(1) Su propósito es gastar el mínimo de poder de combate en esfuerzos secundarios, con el fin de ubicar el máximo poder de combate en esfuerzos principales. (2) La economía de fuerzas es el empleo y distribución juiciosa de las fuerzas. Es la asignación mesurada del poder de combate disponible a tareas tales como ataques limitados, defensa, retrasos, engaño o incluso operaciones retrógradas para lograr una masa en otro lugar en el punto y momento decisivos.
5. Maniobra	El propósito de la maniobra es colocar al enemigo en una posición desventajosa para el mediante la aplicación flexible de potencia de combate. Maniobra es el movimiento de fuerzas en relación con el enemigo con el objeto de asegurar o retener una posición ventajosa, … Contribuye materialmente a la explotación del éxito, a la preservación de la libertad de acción y a la reducción de la vulnerabilidad, presentándole continuamente nuevos problemas al enemigo.	(1) El propósito de la maniobra es colocar al enemigo en una posición de desventaja. (2) La maniobra es el movimiento de las fuerzas en relación con el enemigo para asegurar o retener la ventaja posicional, … Una maniobra eficaz mantiene al enemigo fuera de equilibrio y, por lo tanto, también protege a la fuerza amiga. Contribuye materialmente a la explotación de los éxitos, a la preservación de la libertad de acción y a la reducción de la vulnerabilidad al plantear continuamente nuevos problemas al enemigo.

6. Unidad de Mando	…asegurar la unidad de esfuerzo bajo un comandante responsable para cada objetivo. Unidad de mando significa que todas las fuerzas operan bajo un solo comandante con la autoridad requerida para dirigir a todas las fuerzas empleadas en búsqueda del logro de un propósito común. La unidad de esfuerzo (la coordinación a través de la cooperación y los intereses comunes) es un complemento esencial de la unidad de mando.	(1) …es asegurar la unidad de esfuerzo bajo un responsable para cada objetivo. (2) …significa que todas las fuerzas operan bajo un único comandante con la autoridad necesaria para dirigir todas las fuerzas empleadas en la consecución de un objetivo común. La unidad de mando puede no ser posible con socios multinacionales e interagenciales. La unidad de esfuerzo es la coordinación y cooperación hacia objetivos comunes…
7. Seguridad	El propósito de la seguridad es nunca permitir que el enemigo adquiera una ventaja inesperada. La seguridad optimiza la libertad de acción mediante la reducción de la vulnerabilidad de las fuerzas amigas a actos hostiles, a la influencia o a la sorpresa. Aun cuando los riesgos son parte inherente de las operaciones militares, la aplicación de este principio incluye el manejo prudente de ellos, no la prevención indebida.	(1) El propósito de la seguridad es evitar que el enemigo adquiera una ventaja inesperada. (2) La seguridad aumenta la libertad de acción reduciendo la vulnerabilidad de los amigos a los actos hostiles, la influencia o la sorpresa. …la planificación del Estado Mayor y la comprensión de la estrategia, táctica y doctrina del enemigo aumentan la seguridad….La aplicación de este principio incluye una gestión prudente del riesgo, no una precaución indebida.
8. Sorpresa	El propósito de la sorpresa es atacar al enemigo en un momento o lugar en el cual no esté preparado, o en una forma para la cual no esté prevenido. La sorpresa puede ayudar al comandante a cambiar el equilibrio de la potencia de combate y, de esa manera, lograr el éxito bastante fuera de proporción con el esfuerzo realizado.	(1) El propósito de la sorpresa es atacar en un momento o lugar o de una forma para la que el enemigo no está preparado. (2) (2) La sorpresa puede ayudar al comandante a cambiar el equilibrio del poder de combate y así lograr un éxito muy desproporcionado con respecto al esfuerzo realizado. Los factores que contribuyen a la sorpresa son la rapidez en la toma de decisiones, …la inteligencia eficaz; el engaño; la aplicación de un poder de combate inesperado; la OPSEC; y las variaciones en las tácticas y los métodos de operación.

9. Simplicidad	El propósito de la simplicidad es preparar planes claros y sencillos y órdenes concisas con la finalidad de garantizar la comprensión total. La simplicidad contribuye a las operaciones exitosas, ya que los planes sencillos y las órdenes claras y concisas minimizan las equivocaciones y la confusión.	(1) El propósito de la simplicidad es… planes claros y sin complicaciones y órdenes concisas. (2) La simplicidad contribuye al éxito de las operaciones. Los planes simples y las órdenes claras y concisas minimizan los malentendidos y la confusión. La simplicidad en los planes permite una mejor comprensión y planificación de la ejecución en todos los escalones.

Nota: Tabla y traducciones elaboradas por el autor.

La tabla anterior permite identificar que los principios fueron extraídos casi textualmente de la doctrina norteamericana, aun así, cabe señalar que en la doctrina base se hace mención en varios puntos a los niveles de la conducción o específicamente a la conducción estratégica, por lo que podemos aseverar que los principios de la guerra nacionales tienen aplicabilidad en este nivel, conforme al origen de su definición.

El siguiente paso fue establecer como estos principios de la guerra son aplicables a la Ciberdefensa a pesar de las características del ciberespacio y la intangibilidad que este dominio presenta. Para demostrar lo anterior, se consideró pertinente citar la metodología que usó el Teniente Coronel de la Fuerza Aérea de los Estados Unidos, Steven Cahanin, quien buscaba determinar nuevos principios de la guerra para el ciberespacio, y no la aplicabilidad de los ya descritos. A pesar de lo anterior, utiliza tres premisas básicas para el análisis, que el autor de esta investigación estimó pertinentes para el propósito perseguido. La primera premisa fue que el ciberespacio es un dominio creado por el hombre y lo debemos controlar para las operaciones militares, puesto que afecta transversalmente a los otros cuatro dominios. Segundo; los blancos presentes en el ciberespacio (propios o adversarios) pueden ser fácilmente atacados, generando graves repercusiones y tercero; los avances tecnológicos son tan rápidos que modifican el dominio, por lo que se necesitan ajustes permanentes para mantener la libertad de acción (Cahanin, 2012).

Las tres premisas descritas, hacen mención a características de este nuevo espacio de batalla, pero las diferencias respecto a los otros dominios no son sustanciales como

para tener que redefinir los principios de la guerra, por ejemplo, el dominio aéreo no es creado por el hombre, pero es transversal a todos los otros dominios. Por otro lado, y sustentado en el concepto de las *operaciones basadas en efectos*[45], planteada tras la Guerra del Golfo Pérsico, debido a las nuevas capacidades disponibles, los blancos estratégicos y/u operacionales podían ser afectados directa y gravemente, cambiando el curso de las operaciones y; asociado a lo anterior, la evolución de los ingenios tecnológicos en todos los dominios (drones, armamento inteligente, blindajes reactivos, etc.) obligan a hacer ajustes permanentes para mantener la iniciativa y ganar la libertad de acción.

Conforme a lo anterior, fue factible establecer al menos, que no es necesario por ahora, generar nuevas fórmulas diferentes a las ya establecidas, en atención a que la revolución aparejada a las características del ciberespacio, guardando las proporciones, es similar a lo que significó en; velocidad, transversalidad a los dominios, sorpresa y efectos posibles, la aviación de guerra en su minuto.

En consecuencia y, establecido el marco, a continuación, será necesario identificar la aplicabilidad de los principios de la guerra reseñados para la Ciberdefensa.

Durante la exploración bibliográfica, fue factible acceder además a una monografía del ya citado Mayor Farmer, quién en su revisión de la historia de los principios de la guerra desde *Sun Tzu* hasta la era del ciberespacio, enfoca uno de sus capítulos a la revisión de los doce principios que rigen la doctrina conjunta de los Estados Unidos. De ese trabajo académico se estimó pertinente destacar algunas de sus aproximaciones, coherentes con el objetivo planteado para esta investigación.

Respecto al *Objetivo*, su definición establece que está orientado a "*Dirigir cada operación militar hacia un resultado claramente definido, decisivo y accesible"* (Ministerio de Defensa, 2011. P:51), esta amplia conceptualización puede ser aplicada a un objetivo en cualquiera de los niveles de la conducción. Teniendo en consideración que los objetivos recibidos por el JEMCO provienen del poder político, y este debe proponer una opción de respuesta militar con los medios disponibles, la aplicación de

[45] Las operaciones basadas en efecto cobran relevancia y se sistematizan después de la 1ra Guerra del Golfo Pérsico. Uno de sus percusores es el Coronel de los Estados Unidos David Deptula, quién basado en la nueva tecnología empleada, aviones y cohetería de precisión, desarrolló estos postulados.

las capacidades ofensivas y defensivas de la Ciberdefensa vienen a contribuir a los objetivos establecidos, en ningún caso podría decirse que la definición del *Objetivo* no pudiera aplicar a la persecución de estos a través de la Ciberdefensa.

Reforzando la idea anterior, Farmer plantea la siguiente idea *"Al incluir las capacidades cibernéticas en… una campaña de bombardeo convencional contra un mismo objetivo, el Comandante de una fuerza conjunta puede reducir significativamente el tiempo para lograrlo y cumplir los objetivos estratégicos nacionales identificados por el Presidente"*[46] (Farmer, 2010. p: 32).

Con lo anterior se puede concluir que este principio es totalmente aplicable, pues va asociado al objetivo de la campaña, por lo que las capacidades utilizadas para alcanzar este fin pueden incluir la acción coordinada de los cinco dominios, integrando a la Ciberdefensa.

El principio de *Ofensiva* hace mención en su descripción teórica a *"tomar, retener y explotar la iniciativa… esta es la manera más eficaz y decisiva de lograr un objetivo claramente definido"* (Ministerio de Defensa, 2011. P:51). La tendencia a pensar en los conceptos de tomar, retener y explotar la iniciativa como algo tangible, pueden llevar a pensar que, para la Ciberdefensa, a pesar de ejecutar operaciones ofensivas, éstas irán en contribución a una operación mayor que logre los conceptos descritos. Lo anterior, puede ser rebatido en el sentido que, en este caso la Ciberdefensa, al igual que la aviación puede competir por la libertad de acción en su dominio específico. Contribuyendo así a facilitar la consecución de ese *objetivo claramente definido* que plantea esta conceptualización.

Un ejemplo real de lo anteriormente descrito fue la incursión rusa en Georgia contra estamentos militares y de gobierno, esta operación de *espectro total*[47] denegó el uso del espectro electromagnético, así como el servicio de internet en todo el país. El efecto que la ciber ofensiva rusa logró al cegar y enmudecer a las fuerzas militares de

[46] Traducción realizada por el autor.

[47] Las operaciones de espectro total hacen referencias a la utilización de capacidades militares en forma simultánea en operaciones militares de guerra y aquellas distintas a la guerra. (Estados Unidos, 2001). Traducción realizada por el autor.

Georgia, reduciendo sus capacidades de mando y control, contribuyó a la victoria en el plano del dominio terrestre y finalmente de la campaña (Farmer, 2010).

Queda de manifiesto que el principio de *ofensiva* puede ser aplicado en forma independiente en cada uno de los dominios, y que las fuerzas asociadas a estos estarán en disputa de esa libertad de acción, que finalmente quién la mantenga y explote, logrará coadyuvar con sus efectos a la consecución del objetivo deseado.

El siguiente principio analizado es *Concentración* (mass), su definición en la doctrina establece en términos generales que se refiere a *"concentrar los efectos de la potencia de combate en un lugar y momento que permitan que la fuerza logre resultados decisivos"* (Ministerio de Defensa, 2011. P:51), además hace referencia que incluso, de contar con un balance inferior de fuerzas totales, la concentración de estas fuerzas en un punto decisivo y por un tiempo poco prolongado puede lograr efectos favorables a la fuerza inferior.

Considerando las características del ciberespacio, sin límites territoriales, donde el tiempo es irrelevante por la velocidad casi instantánea de los movimientos y, los adversarios pueden causar los mismos efectos dañinos con bajo costo referido a los equipos utilizados, es el escenario donde más que nunca, se debe considerar el principio de *concentración*, considerando que las capacidades no son infinitas y no se puede atacar todo ni defender todo al mismo tiempo. Por lo tanto, los comandantes de las fuerzas conjuntas deberán priorizar, conforme a su intención, donde y cuando concentrar la fuerza de la Ciberdefensa, como acción principal o como una acción del mando que apoya.

Un aspecto relevante, que se puede rescatar de la monografía del Mayor Farmer, es lo que expresa respecto a la *aproximación operacional,* estableciendo que *"Un comandante moderno considera en su enfoque operacional todos los dominios, incluidos el aéreo, el terrestre, el marítimo, el espacial y el cibernético, para decidir en qué dominio quiere enfrentarse al enemigo mediante la aplicación de la concentración"* (Farmer, 2010. p:36). Esta frase hace mención en el contexto del *Diseño Operacional*, que primero, se deben considerar todos los dominios de la guerra y segundo, que la *concentración* puede ser aplicada en cada uno de ellos. La aseveración anterior, permite reafirmar que este principio de la guerra es aplicable a la Ciberdefensa.

En el mismo orden de ideas en que se han tratado los principios anteriores, la *Economía de Fuerzas,* por definición doctrinaria establece que *"su propósito es gastar el mínimo de poder de combate en esfuerzos secundarios, permitiendo aumentar el poder en esfuerzos principales"* (Ministerio de Defensa, 2011. P:51) podría confundirse con el principio de *concentración,* pero en este caso el sentido es que la fuerza se debe utilizar por completo, buscando contener con el mínimo de ella aquello que es secundario, priorizando fuerzas en el punto decisivo.

Desde el punto de vista de la Ciberdefensa este principio aun es aplicable conforme lo plantea Leonhard en su obra *Los Principios de la Guerra en la Era de la Información*. Si bien en la mayor parte de este libro se impulsa a la creación de nuevos principios para el ciberespacio, en el caso de la *economía de fuerzas,* hace un guiño asintiendo que en los tiempos modernos los costos en las operaciones, tanto en vidas humanas como en recursos del Estado son altamente criticados, por lo cual, utilizar las capacidades de la Ciberdefensa en esfuerzos secundarios, para priorizar las operaciones que no pueden ser cumplidas de otra manera que no sea la convencional, es donde el principio citado cobra alto valor para la Ciberdefensa (Leonhard, 1998).

Por otro lado, el principio de *Maniobra*, por definición establece que *"El propósito …es colocar al enemigo en una posición desventajosa… Contribuye materialmente a la explotación del éxito, a la preservación de la libertad de acción y a la reducción de la vulnerabilidad, presentándole nuevos problemas al enemigo"* (Ministerio de Defensa, 2011. P:51). Así como en los otros principios el concepto puede ser aplicado a cualquier nivel de la conducción y, para el caso particular de la investigación, la maniobra estratégica debe venir a contribuir a través del uso del poder militar de la nación, a una posición ventajosa sobre un adversario, obligándolo a desistir del uso de la fuerza o de la persistencia de sus hostilidades. En ese contexto, se debe considerar que el adversario posee capacidades similares en el ciberespacio más que en otros dominios, por lo que el ingenio militar debe aprovechar las vulnerabilidades de este para maniobrar a su favor.

Un claro ejemplo de lo anterior, lo plantea Farmer al ejemplificar con el corte de un cable subterráneo de fibra óptica el año 2009 en Egipto, el que generó la suspensión parcial del servicio de internet en parte de India y prácticamente todo el Medio Oriente.

Se desconoce la autoría, pero el hecho es que, a través de un ataque físico en el espectro de las operaciones de información, se configuró un escenario para aquellas fuerzas que poseían internet satelital, dando tiempo y espacio por sobre el adversario. Farmer, lo compara con una acción directa sobre un puente que obliga a cambiar de dirección a las fuerzas en movimiento, exponiéndolos a nuevas vulnerabilidades, retrasándolos y paralizando en parte, su ciclo de decisiones.

Todo lo anterior permitió evidenciar que, al pensar en Ciberdefensa, no se puede limitar a los datos y acciones en la red intangible, ella puede maniobrar en cualquiera de las capas que componen el ciberespacio; infraestructura crítica, datos, redes e incluso el personal. Se puede afirmar que el principio de *maniobra,* en la Ciberdefensa, está totalmente vigente.

La *Unidad de Mando,* es entendida como *"asegurar la unidad de esfuerzo bajo un responsable para cada objetivo… todas las fuerzas operan bajo un único comandante con la autoridad necesaria para dirigir todas las fuerzas empleadas en la consecución de un objetivo común"* (Ministerio de Defensa, 2011. P:52). Esta definición, entendida desde la filosofía de las operaciones militares conjuntas, tiene cabida plena en cada uno de sus dominios. En el caso de Estados Unidos, la creación del *CyberCommand* es la mejor muestra de que las acciones en el quinto domino de la guerra, dependen de la coordinación de esfuerzos bajo un mando único.

Desde el punto de vista de la sinergia que se debe lograr en las operaciones, el caso de la Ciberdefensa puede ser vista desde dos perspectivas, primero; en el ámbito general de la maniobra, adherir a la unidad de mando permitirá evitar las interferencias mutuas con los otros dominios, siendo altamente eficiente en el aporte específico a la consecución de los objetivos y, segundo; en lo específico del quinto dominio, la capacidad del Comandante Conjunto o del JEMCO de contar con la disponibilidad de las capacidades de todas las FAs, bajo un solo esfuerzo coordinado, le entrega una herramienta para generar efectos de repercusiones estratégicas.

Respecto a lo anterior y en palabras de Farmer *"El USCYBERCOM, … proporcionará la estructura requerida para garantizar que el mando y control sean mantenidos por y para las fuerzas amigas. Estos esfuerzos son un testimonio de validez del principio de unidad de mando en un contexto cibernético"* (Farmer, 2010. p: 42).

Por otro lado, el propósito del principio de *Seguridad* es descrito por las doctrinas como *"nunca permitir que el enemigo adquiera una ventaja inesperada… optimiza la libertad de acción mediante la reducción de la vulnerabilidad de las fuerzas amigas a actos hostiles, a la influencia o a la sorpresa"* (Ministerio de Defensa, 2011. P:52). Esta definición cobra gran vigencia en el ámbito del ciberespacio, ya que no se puede desconocer la génesis de la Ciberdefensa a nivel nacional, que emerge como una necesidad de ampliar los conceptos de ciberseguridad en el sector de la Defensa Nacional. El propósito es garantizar el uso libre y seguro del ciberespacio para la población, y para la Ciberdefensa, resguardar la soberanía nacional en este dominio.

Lo anterior, nos permite identificar que solo por definición el principio de *seguridad* tiene validez. Gran parte de los esfuerzos de las naciones es proteger su red nacional de infraestructura crítica y la Defensa no está ajena a esto. Así como hemos tomado el ejemplo de Estados Unidos, es posible encontrar declaraciones como la de *CBS News,* que exponían el 2009:

> Las fuerzas de Ciberdefensa deben mantener una vigilancia constante del dominio cibernético en busca de posibles amenazas. Las autoridades estadounidenses deben adoptar estas medidas de seguridad para evitar que ocurra un ciber Pearl Harbor a la nación. Las entidades de ciber estadounidenses ya han sorprendido a las fuerzas de ciberespionaje rusas y chinas realizando reconocimientos de la red eléctrica de Estados Unidos[48]. (CBS, 2009)

El principio de seguridad, tal vez, es uno de los más fáciles de identificar y describir en el ámbito de la Ciberdefensa. Contar con sistemas protegidos y con la disponibilidad de datos, información e infraestructura crítica asociada, indudablemente permitirá contar con la libertad de acción para actuar cuando sea requerido.

Otro de los principios de la guerra analizado es la *Sorpresa,* su definición doctrinaria establece que su propósito es *"atacar al enemigo en un momento o lugar en el cual no esté preparado…puede ayudar a cambiar el equilibrio de la potencia de combate…,*

[48] Traducción realizada por el autor.

lograr el éxito fuera de proporción con el esfuerzo realizado" (Ministerio de Defensa, 2011. P:51). Este principio es uno de los más antiguos y ciertamente aun aplicable a cualquiera de los dominios, incluido el ciberespacio. Estrategas referentes como Sun Tzu en su obra *El Arte de la Guerra,* establece en su capítulo primero de *las estimaciones "toda la guerra se basa en el engaño… por eso cuando seas capaz, finge incapacidad; cuando estés activo, finge inactividad; cuando estés cerca, aparenta estar lejos… cuando no esté preparado; haz incursiones cuando no te espere"* (Griffiths, 2005. p: 100), o bien el mismo Clausewitz en su obra *Principles Of War:*

> Juega un papel mucho más importante en la estrategia que en la táctica. Es el elemento más importante de la victoria. Napoleón, Federico II, Gustavo Adolfo, César, Aníbal y Alejandro deben los rayos más brillantes de su fama a su rapidez. (Clausewitz, en Farmer, 2010. p:44)

Como ha sido expuesto, la sorpresa concebida en el pasado está plenamente vigente en el presente del quinto dominio de la guerra, condiciones como; velocidad, secreto, confidencialidad, no autoría, son características que permiten a la Ciberdefensa accionar en el más alto nivel de la conducción, explotando el factor sorpresa.

Para poder ejemplificar lo anterior, es factible nombrar a Rusia y el factor sorpresa alcanzado frente a Estonia el año 2007:

> …la interrupción de los servicios afectó a todos los ciudadanos, enviando un mensaje muy claro al pueblo estonio por parte de sus antiguos amos rusos. Al ser el primer ciberataque documentado contra una nación, los rusos no sólo sorprendieron a Estonia, sino también a la OTAN y a Estados Unidos. (Ashmore en Farmer, 2010. p:45)

Lo anterior nuevamente permitió identificar la aplicabilidad del principio de la *sorpresa* en el ciberespacio, articulada por las capacidades que ofrece la Ciberdefensa, más que en cualquier otro de los dominios.

Por último, el principio de *Simplicidad* por definición y en términos generales, establece claramente que su propósito es *"preparar planes claros y sencillos y órdenes concisas con la finalidad de garantizar la comprensión total"* (Ministerio de Defensa, 2011. P:51).

Lo descrito no permite mucha interpretación, este postulado, así como la sorpresa también fue tratado por Clausewitz en una frase muy decidora; *"en la guerra todo es simple, pero lo más simple es difícil"* (Clausewitz, en Farmer, 2010. p:45).

Manteniendo la discusión en el nivel más alto de la conducción, y volviendo a la naturaleza de los problemas más complejos, es fundamental que la planificación y las coordinaciones en este nivel se mantengan sencillas, más aún para un dominio que es transversal a los otros cuatro (tierra, aire, mar, espacio). Caer en el agobio de los aspectos técnicos y tecnológicos de la Ciberdefensa, para muchos, puede dejar el principio de la *simplicidad* totalmente fuera de esta ecuación, pero al nivel estratégico no le compete esa complejidad, más bien le corresponde comprender, que se posee una herramienta poderosa para configurar una opción de respuesta militar, ello demanda con mayor énfasis al conductor estratégico, concebir este empleo lo más simple posible en términos de coordinaciones y efectos deseados.

Para reforzar lo anterior, es posible manifestar lo siguiente:

> …manteniendo la conducción de las ciberoperaciones simples, se puede ayudar a reducir los elementos potenciales de fricción que inevitablemente ocurren cuando el mejor plan trazado entra en contacto con la realidad; una ciber operación simple, integrada en una operación más grande del comandante de la fuerza conjunta puede ayudar a lograr los resultados deseados. (Farmer, 2010. p: 46).

Nuevamente fue posible establecer que existe una aplicabilidad plena de los principios de la guerra para la Ciberdefensa, concebida desde el más alto nivel de la conducción. A juicio del autor no es una virtud de la Ciberdefensa, muy por el contrario, todo el mérito es para los estrategas y teóricos militares que pudieron desmembrar la complejidad de la guerra y concebir elementos tan amplios, que puedan ser aplicados indistintamente la evolución del tiempo y la tecnología. Es por lo anterior que, el conductor estratégico debe comprender la poderosa herramienta técnica y tecnológica que posee, y como ella se desenvuelve en el quinto dominio de la guerra.

Además de lo anterior, la responsabilidad del conductor estratégico será complementada y potenciada por el trabajo de su Estado Mayor, quienes deberán

“tener una clara idea general de los principios de la guerra en relación con la situación que se vive, dado por su juicio profesional” (Rivas, 1968. p:10).

Por último, y para finalizar el análisis de este factor, fue considerado como un aporte hacer mención a las palabras de cierre concebidas por el Mayor Farmer en su monografía, su trabajo de revisión histórica e interpretación facilitaron la comprensión de los principios extraídos de la doctrina norteamericana, por lo que es pertinente señalar:

> La durabilidad de los Principios de la Guerra es un testimonio de su utilidad. Los principios se definen con la suficiente amplitud como para que sean aplicables al entorno operativo actual y, sin embargo, son lo suficientemente específicos como para ser aplicados en todos los niveles de la guerra. (Farmer, 2010. p:52)

4.4 Resultados del capítulo

En el presente punto, se exponen los resultados obtenidos luego del análisis de los factores seleccionados para el estudio de la Ciberdefensa y su nexo con el nivel estratégico. Por una parte, fueron analizadas las variables estratégicas *militar, infraestructura e informaciones* como parte del conjunto de las PEMSII-PT e identificado el comportamiento de la Ciberdefensa. Por otro lado, se examinó la aplicabilidad de los *Principios de la Guerra* declarados por la Doctrina Nacional Conjunta, buscando identificar la vigencia de aplicación de estos principios en el quinto dominio de la guerra.

Respecto a las variables PEMSII-PT, se estimó pertinente establecer el marco por el cual fueron seleccionadas como variables de análisis estratégico en la doctrina nacional y se confrontó con la doctrina base de los Estados Unidos y la OTAN. Establecido lo anterior y, aceptado que para el estudio del campo de batalla se deben considerar el impacto de los cinco dominios de la guerra en las variables PEMSII-PT, se demostró a través de los datos obtenidos en un estudio de simulación de un ambiente operacional complejo, como la Ciberdefensa afectaba a estas variables.

A través de este estudio específico, fue posible identificar el comportamiento de la Ciberdefensa a la luz de PEMSII-PT y concluir de esta manera que los efectos generados en las variables *militar, informaciones e infraestructura*, son atingentes a los problemas estratégicos.

Por otra parte, respecto a la aplicabilidad de los principios de la guerra, la estructuración del capítulo permitió hacer una breve reseña de su significado, a juicio del autor y, con la experiencia obtenida en la investigación, se puede afirmar que, al adentrarse en la descripción de estos, es conveniente comprender su conceptualización, más que buscar una definición absoluta.

En el desarrollo del capítulo, se demostró que los principios de la guerra conjuntos son extraídos prácticamente textuales de la doctrina de los Estados Unidos, por lo que se plasmó una tabla comparativa, que sirvió de base para el análisis de estos en el ambiente operacional estratégico conjunto.

Los principios de la guerra fueron tratados uno a uno, primero; buscando a través de la comprensión de la filosofía de estrategas y pensadores militares y; segundo, con ejemplos aplicados en conflictos del último siglo, demostrar la aplicación al contexto del quinto dominio de la guerra, pudiendo a ciencia cierta comprobar que los amplios lineamientos en cómo éstos están concebidos y la lógica que subyace a su aplicación, son totalmente aplicables al empleo de la Ciberdefensa.

4.5 Validación de los resultados

Conforme a la experiencia de los especialistas, y principalmente a la luz del propósito de dos propósitos de la entrevista: 1) Identificar uso de las variables PEMSII-PT y/o agregar alguna otra, y 2) Aplicabilidad de los Principios de la Guerra Conjuntos para la estructuración de la maniobra de Ciberdefensa; se pudo hacer la triangulación necesaria para concluir respecto a cuál es el comportamiento de la Ciberdefensa a la luz de las variables de análisis estratégicas PEMSII-PT y además la aplicabilidad de los *Principios de la Guerra Conjuntos.*

Tabla 8 Opinión de expertos: Aplicabilidad de los Principios de la Guerra Conjuntos para la estructuración de la maniobra de Ciberdefensa

Objeto de la pregunta	Especialista	Información obtenida
¿Otra variables además de PEMSII-PT?	GDD GRIFFITHS	"variables culturales y sociales, idiosincrasia, sin duda la variable legal es clave, el oficial de Estado Mayor debe ser formado en forma integral, necesidad de entender el contexto en el que se usa la fuerza" (4:30) "Las variables, no son dogma de fe, se deben incorporar todas las variables necesarias"
	GDD PINO	Sin duda hay que mantener siempre presente el tema legal, hoy en día no se puede dejar de lado (20:19), no solo es necesaria, es hasta innovadora en el ámbito de la ciber defensa.
	GDD VARELA	No olvidar que PEMSII viene de la doctrina OTAN, por lo que hay que entender que la doctrina hay que adaptarla a diferentes metodologías de análisis. Pero es eso una metodología. (4:40) La generación del JEMCO permite adaptar estas metodologías, pero finalmente la conclusión es que hay que agregar los factores necesarios para dar un buen entendimiento del ambiente. (05:54) El mundo de la Ciberdefensa hoy marca un cambio tan radical como el uso del espacio aéreo el siglo pasado (6:49), hay que entender que la ciber no responde ni a fronteras ni a leyes y las leyes que existen van asociadas a delitos (7:32). Este escenario es anárquico, y hay que poder operar en él.
	GDB GREZ	No hay que perder de vista que las variables PEMSII son una herramienta de varias más que existen, si bien la doctrina nacional propone esta herramienta de análisis no hay que olvidar que la doctrina es una guía, por lo que hay variables como las legales, culturales, coyunturales de cada problema. Me inclino por decir que las variables PEMSII son la base y deben ser complementadas por lo legal y todo aquello que, considerando el tiempo disponible, aporte a una comprensión del problema y a la toma de decisiones.
	CRL VERA	Creo que variables son múltiples y además que si la doctrina sugiere esa metodología no es una caja cerrada, es decir, la doctrina sugiere el desde. Yo le agregaría aspectos sociales y legales. Como lo que estamos viendo hoy en Ucrania.
	CRL MELENDEZ	La variable legal debe ser considerada, el Manual de Tallin para las naciones de la OTAN es una muestra de ello, no se puede omitir en ningún caso este aspecto a pesar de que exista la capacidad de repudiar un ataque.

Objeto de la pregunta	Especialista	Información obtenida
	CF SIÑA	Creo que, desde el punto de vista de la Ciber, es el desde la metodología PEMSII, hoy que agregar toda aquella que pueda afectar en sus efectos al Estado, lo que sean necesario. Lo legal por supuesto, lo social, la infraestructura crítica, lo importante es que esto sea centralizado en la planificación del EMCO y no cada uno por su lado.
	TCL VILLARROEL	Para comprender el ambiente operacional, los factores de análisis son más amplios y variables, excediendo en muchas oportunidades a los comúnmente estudiados PMESII-PT, pudiendo efectivamente integrar aspectos legales, o, como menciona la doctrina de Inteligencia de Naciones Unidas, factores Culturales, Históricos y Religiosos (PMERSCHIIPT) y eventualmente otros (como en el caso del despliegue de capacidades en apoyo al EEC-C por la Pandemia, la inclusión de un factor sanitario). En este sentido, es relevante que un conductor militar expuesto a problemas complejos y mal estructurados debe tener la capacidad de integrar todas las variables posibles (en el tiempo disponible) y no limitarse exclusivamente conocido.
Aplicabilidad de los Principios de la Guerra Conjuntos para la estructuración de la maniobra de Ciberdefensa	GGD. GRIFFITHS	"La guerra no ha cambiado en su naturaleza, pero si en su carácter, por lo que creo que se deben volver a revisar los principios de la guerra para esta dimensión, porque los principios de la guerra han sido levantados sobre las tres dimensiones, no quiere decir que no sirven, por el contrario, son aplicables algunos y sin duda aparecerán otros en la medida que se adquieran experiencias de su empleo" (23:43)
	GDD PINO	Los principios son una guía y creo que donde operan fuerzas militares independiente de su categoría se pueden utilizar los principios en forma genérica, tal vez con esta dimensión hay que ajustar algunos, pero la respuesta final es sí.
	GDD VARELA	Como son principios son referenciales, y dan criterios de éxito, y como son genéricos aplican, tal vez no todos, pero lo más importante es que se pueden crear nuevos conforme a las características de la ciber (17:10)
	GDB. GREZ	Todos, creo que este dominio y en concordancia con la aplicabilidad a la maniobra estratégica, los principios de la guerra son aplicables y no descarto que puedan aplicarse cosas nuevas desde el punto de vista de la temporalidad. Lo más discutible puede ser la mantención del terreno, pero si lo piensas también se debe contar con un dominio de las redes y nunca perder de vista la dimensión física del ciberespacio.
	CRL VERA	Son aplicables, creo que hay que tenerlos presentes, pero también en este ámbito hay que dejar de lado los límites espaciales y la concentración de fuerzas a veces se pierde, lo dejaría como concentración de esfuerzos.

Objeto de la pregunta	Especialista	Información obtenida
	CRL. MELENDEZ	Son aplicables, la mejor explicación es que son un principio de optimización, son principios generales para tener en cuenta para concebir la maniobra ciber. De tal manera de asegurar una maniobra optimizada, no es dogma es una guía para acercarse a lo óptimo
	CF SIÑA	Claramente, si o si debe incluirse la metodología de planificación bajo los principios de la guerra conjuntos.
	TCL. VILLARROEL	Los principios de la guerra son totalmente válidos y aplicables para toda Operación Militar de Guerra, tanto para el empleo de la capacidad de Ciberdefensa como parte de una maniobra conjunta (que integre distintas capacidades), como en una Operación exclusiva de Ciberdefensa.
	CRL. BURBANO	Si, son aplicables en especial: Flexibilidad, oportunidad, iniciativa, disuasión, economía de fuerzas.

Nota: Tabla elaborada por el autor.

A la luz de los resultados de la exploración doctrinaria, que dio el marco de comprensión del comportamiento de la Ciberdefensa en las variables de análisis estratégicas, y la identificación de la aplicabilidad de los principios de la guerra del nivel conjunto, así como en cada capítulo de la investigación y con el fin de saturar los datos y validar los resultados mencionados, es que los especialistas consultados entregaron aportes significativos a la investigación.

En primer término, respecto a las variables PEMSII-PT, los especialistas destacaron primero que es una metodología adoptada y que como tal, debe ser analizada sin restarse a otras miradas, además de lo anterior, expresan casi unánimemente que deben ser considerados tantos factores como sean necesarios para cumplir el fin que busca: comprender el problema estratégico.

Otro factor común es la inclusión de las variables legales que implica el uso y las operaciones en el ciberespacio, alguno de los especialistas pone énfasis incluso en el Manual de Tallin, vigente para las naciones de la OTAN, por lo que se puede concluir que las variables PEMSII-PT deben ser consideradas como la metodología de análisis del ambiente operacional que enmarca el problema estratégico, pero el hallazgo principal en la conversación con los especialistas, es que debe ir ampliándose en

aspectos, sociales, culturales y legales, donde la Ciberdefensa impacta y genera efectos estratégicos, operacionales y tácticos.

Por otro lado, y desde la mirada de los principios de la guerra conjuntos, fue factible ver la concordancia de todos los especialistas en la aplicabilidad de éstos al referirnos a la Ciberdefensa. Algunos de ellos incluso no descartan la posibilidad de que aparecieran nuevos, y que alguno de los actuales pudiese dejar de aplicarse en el quinto dominio de la guerra. Esa discusión también fue encontrada en la doctrina, pero la consonancia de los especialistas radica, en la filosofía en cómo están concebidos, que su carácter de genéricos permite su aplicación, manifestando además, que deben ser una guía y no *"dogma de fe"* como indica el General Griffiths. Por último, se resalta el concepto usado por el Coronel Meléndez quien los interpreta como *"un principio de optimización"*, es decir, que tenerlos considerados para enfrentar los desafíos de las operaciones militares en cualquiera de los dominios, permite optimizar los medios y modos disponibles conforme a los fines deseados y/o impuestos.

En atención a todo lo anterior, se pudo concluir que la información rescatada de los textos doctrinarios, así como de estudios y publicaciones militares, son coherentes con la experiencia de campo de los especialistas, lo que permitió al autor reforzar la convicción que ambos objetivos planteados para el presente capítulo, por un lado la identificación del comportamiento de la Ciberdefensa a la luz de las variables de análisis estratégicas y, por otro la aplicabilidad de los principios de la guerra establecidos en la doctrina conjunta, han sido alcanzados en los términos de rigurosidad esperada en la investigación.

4.6 Síntesis del capítulo

El propósito del capítulo fue determinar, por un lado, el comportamiento de la Ciberdefensa bajo la metodología de análisis de las variables estratégicas PEMSII-PT y, por el otro la aplicabilidad de los *Principios de la Guerra* del nivel conjunto en la acción de la Ciberdefensa.

Para abordar el primer objetivo, la metodología se basó primero en acotar las variables PEMSII-PT, solamente a aquellas *militar, infraestructura e informaciones,* para a través

de la revisión bibliográfica primero; establecer por qué estas son las variables utilizadas en el nivel estratégico y; posteriormente a través de los resultados de un ejercicio de simulación, poder identificar el comportamiento de la Ciberdefensa a la luz de estas variables de análisis.

La segunda parte del capítulo estuvo orientada a determinar la aplicabilidad de los principios de la guerra conjuntos respecto al uso de la Ciberdefensa. En un primer momento se conceptualizó el término; luego se confrontaron en un resumen las definiciones de la Doctrina Nacional Conjunta contra su homólogo de los Estados Unidos; para finalmente, a través de ejemplos y posturas fundadas en estudios realizados, así como la apreciación doctrinaria del autor, determinar la aplicabilidad de estos principios a la Ciberdefensa.

Por último, se realizó la validación de los resultados a través de las deducciones de las entrevistas a especialistas, que a través de sus posturas y declaraciones permitieron validar aquellos antecedentes extraídos de la doctrina, tanto para la discusión de las variables estratégicas, como para los principios de la guerra, permitiendo al autor concretar ambos objetivos planteados para este capítulo.

CAPÍTULO V
CONCLUSIONES Y PROPUESTAS

5.1 Conclusiones

Durante el desarrollo del presente capítulo, se exponen las conclusiones obtenidas como resultado de lo expuesto en el trabajo de investigación. Para lo anterior, se realizó una síntesis capitular vinculada a cada uno de los objetivos parciales de la investigación, dando respuesta a las preguntas específicas, y consecuente con ello al objetivo de la investigación.

Además de la síntesis capitular, se realizó una valorización del trabajo investigativo, sustentado en un juicio crítico que permitió resaltar todos aquellos aspectos positivos que permitieron llevar a cabo la investigación, así como las dificultades que de una u otra manera, influyeron como obstáculos en la determinación de los resultados finales.

Finalmente, se realiza una proposición derivada de los resultados obtenidos, exponiendo algunas brechas o vacíos conceptuales que permitirían vislumbrar futuras líneas de investigación.

5.1.1 Síntesis

En el capítulo I *"Problema de investigación",* se establece la problematización, realizando una breve síntesis del estado del arte respecto a los conceptos relacionados con el ciberespacio, ciberdefensa, ciberoperaciones, así como el panorama de la situación de Chile, respecto al marco legal que regula y dispone el marco de la Ciberdefensa en el sector Defensa. En ese contexto se dio origen al cuestionamiento respecto a que si la Ciberdefensa es un problema estratégico, pero la respuesta dicotómica a ese planteamiento lleva a obtener una primera conclusión y plantear indudablemente que sí.

Con ese primer supuesto, es que surgió el cuestionamiento y planteamiento del problema de investigación: ¿Por qué la Ciberdefensa constituye un problema estratégico en la conducción militar?, lo que origina consecuentemente el objetivo

principal del presente trabajo, que fue determinar las características de la Ciberdefensa que la determinan como un problema de la conducción estratégica. Es consecuente con ello, que el desarrollo de los capítulos posteriores se enfoca en dar respuesta a objetivos parciales como es explicado en párrafos posteriores.

El capítulo primero, además de establecer el problema de investigación, recorre paso a paso el proceso metodológico, dando validez a la estructura desarrollada posteriormente, estableciendo claramente los límites del trabajo, así como los procedimientos para dar cumplimiento al rigor científico exigido. Se puede inferir, a partir de este primer apartado, que el éxito en el cumplimiento de los objetivos secundarios, y finalmente el objetivo de la investigación, radica en gran parte en la estructura metodológica sólida planteada en el capítulo primero.

Por su parte el capítulo II *El problema estratégico,* tuvo por objeto la determinación del concepto *problema estratégico*, puesto que, en la Doctrina Nacional Conjunta, no existe una definición tal que permitiera asociar las características de la Ciberdefensa a este nivel de la conducción.

La metodología utilizada fue primeramente deductiva, descomponiendo el concepto en dos partes: *el problema militar* y *nivel estratégico.* El tratamiento de estos conceptos por separado bajo la mirada de las doctrinas de Chile, Colombia, España, Estados Unidos y, Reino Unido, permitió en una primera instancia de análisis, extraer todas aquellas características o adjetivos calificativos del problema en estas doctrinas, donde se pudo evidenciar que al menos el *problema militar* en el alto nivel era: mal estructurado, incompleto, mal definidos, complejos, inciertos, interconectado, dinámico, multidisciplinario, ambiguo, adaptativo y, de tratamiento bajo metodología de análisis.

Por su parte el nivel estratégico, fue analizado bajo las mismas doctrinas mencionadas, llegando a términos más homólogos que el caso anterior. Un hallazgo importante del ejercicio analítico, fue la comprensión comparada con Estados Unidos y aquellos países o alianzas que poseen un nivel de la conducción menos respecto de Chile, o que acuñan el concepto de *gran estrategia*, haciendo referencia a las decisiones políticas de la nación. Para el nivel estratégico de la conducción se obtuvieron las siguientes características: articula modos y medios para alcanzar fines políticos, es del

más alto nivel militar, se conjuga con otros elementos del poder nacional (económico, diplomático, informaciones), se concentra bajo un mando único, concentra la totalidad de las ramas de la Defensa de la nación, posee metodología de solución de problemas y planificación de Estado Mayor, sus productos conforman los planes de los niveles operacionales y tácticos, puede articularse en forma multinacional y utiliza perspectivas a largo plazo y supuestos para la solución de sus problemas.

Una vez descompuesto el problema en partes y obtenidas las características de ambos, se invirtió la lógica de la metodología, y a partir de las partes se construye un término general, siendo posible por parte del autor, conceptualizar el *problema estratégico* como:

> Dilema del ámbito militar de más alto nivel, que se interpone entre la situación actual y los objetivos esperados por el Estado que, por las características de complejidad, incertidumbre, dinamismo e interdependencia, demandan de una metodología de análisis de variables múltiples para aproximarse a su naturaleza, permitiendo así establecer una opción de respuesta, empleando el poder militar de la Nación[49].

La definición de este constructo propio, sumado a las opiniones vertidas por especialistas en la investigación de campo, permitió dar cumplimiento al primer objetivo parcial de la investigación, pudiendo distinguir que es un problema estratégico, dando paso a los capítulos venideros para la descripción, identificación y aplicabilidad de las características de la Ciberdefensa enmarcado en este contexto.

El capítulo III *El 5to domino de la guerra y la Ciberdefensa,* tuvo como propósito describir las características estructurales de la Ciberdefensa en el contexto del 5to dominio de la guerra. Fue así como la investigación identificó como Chile y las doctrinas referentes han considerado y conceptualizado el Ciberespacio y la Ciberdefensa. A partir de estas características, fue posible asociar el estrecho vínculo con el más alto nivel de la conducción militar.

[49] Definición elaborada por el autor.

Previo a profundizar en la exploración específica de las características estructurales, se estimó pertinente tomar aspectos del marco teórico referido al ciberespacio y ampliar su comprensión como 5to dominio de la guerra. A partir de esta aproximación teórica, los esfuerzos estuvieron dados por una metodología descriptiva, en la identificación de: la definición, el propósito que busca, su responsable o encuadramiento en el Estado, el marco legal o regulatorio que la rige, sus principios o componentes y el alcance de interacción en fuerzas armadas, interagencial o intersectorial.

Respecto de lo anterior, y tras el análisis de cada una de las doctrinas seleccionadas, así como las opiniones de los especialistas, se identificaron con creces las características de la Ciberdefensa, pudiendo concluir, por ejemplo, que su *definición* viene en términos generalmente relacionados con la mitigación de riesgos y amenazas en el ciberespacio que puedan afectar los intereses nacionales. Por su parte en cuanto al *propósito*, la tendencia es asegurar la libertad de acción en este dominio. Respecto al encuadramiento, las doctrinas primero; lo sitúan en el sector Defensa segundo; independiente de la unidad (Comando Conjunto, Dirección o Departamento), dependen del Ministerio de Defensa y por sobre las instituciones, servicios o ramas, adquiriendo en todos los casos connotación conjunta. Tanto el marco regulatorio como principios fundamentales están tratados en todas las doctrinas con ciertas diferencias, pero con puntos en común a la doctrina de operaciones en cualquiera de los otros dominios, y por último; hay consenso que su alcance es interagencial.

Con todo lo anteriormente expuesto, fue factible dar cumplimiento al propósito del capítulo, quedando identificadas las características estructurales de la Ciberdefensa y, con ello tributando al objetivo principal de la investigación.

El capítulo IV Las variables operacionales y los principios de la guerra, tuvo el propósito de dar respuesta a las dos últimas preguntas subsidiarias de la investigación. La primera de ellas el comportamiento de la Ciberdefensa a la luz de las variables PEMSII-PT, y la segunda la posible aplicabilidad de los principios de la guerra en el 5to dominio. A diferencia de los capítulos anteriores, en esta oportunidad no se buscó realizar un análisis comparado de las doctrinas seleccionadas, sino que el enfoque estuvo basado en la determinación del detalle que consideraba cada variable en el contexto de la

Ciberdefensa, utilizando la doctrina de los Estados Unidos, así como publicaciones militares afines y resultados de estudios de simulación.

Para cumplir el objetivo, identificar el comportamiento de la Ciberdefensa, el primer paso fue acotar las variables de análisis, poniendo el énfasis en lo militar, las infraestructuras, y las informaciones. Seguido de lo anterior, se estableció cómo puede afectar la Ciberdefensa en cada una de las variables y por último, a través de los resultados de un ejercicio de simulación, lograr identificar claramente los efectos de la Ciberdefensa en ellas, pudiendo así cumplir el objetivo planteado, y más importante aún, identificar el impacto de los efectos de la Ciberdefensa en un nivel de decisiones gubernamentales y estratégicas.

Por su parte, los principios de la guerra fueron acotados a aquellos que establece la Doctrina Nacional Conjunta, pudiendo establecer primero; que son extraídos prácticamente textuales de la doctrina norteamericana, y segundo que independiente de la doctrina o las publicaciones revisadas, los principios no se pueden definir como tal, más bien deben conceptualizarse como un método de optimización de los medios y modos, conforme a los fines deseados.

En la exploración, se expuso como la Ciberdefensa es aplicable a cada uno de los nueve principios de la guerra, analizada desde la perspectiva del nivel estratégico, esa inferencia vino reforzada por la experiencia de los especialistas donde, en sus afirmaciones y opiniones, se pudo llegar al consenso de que son aplicables a esta y no se cierran a la posibilidad de que incluso, pudieran surgir nuevos.

Habiendo cumplido uno a uno los objetivos intermedios, es factible establecer que, a través del presente trabajo de investigación, se pudo validar el postulado inicial de que la Ciberdefensa es un problema del nivel estratégico, pero más importante aún, se logró identificar todas aquellas características que la identifican como un problema militar en el nivel más alto de la conducción.

5.1.2 Valoración

Durante el desarrollo de la presente investigación, el autor considera de gran valor algunos aspectos tratados en el proceso de análisis de la información, pero además,

reconoce aspectos que dejan a la vista debilidades que a primera vista, y con la maduración de los conceptos, podrían ser subsanadas.
La primera fortaleza observada, fue la estructuración del problema de investigación y la delimitación establecida, puesto que, en el ámbito de la Ciberdefensa y Ciberespacio, existe una gran proliferación de posturas y conceptos que podrían haber llevado la investigación a complejizarse, más allá de lo esperado.

Otro factor positivo fue la capacidad de desarrollar los conceptos nucleares, haber podido confrontar diferentes doctrinas y puntos de vistas académicos, para finalmente construir términos propios del autor para ser aplicados en la investigación. Se estima que la gran amenaza de no contar con consensos académicos respecto a algunos conceptos, fue transformada rápidamente en una oportunidad y explotada capítulo a capítulo, contando con un marco teórico robusto, permitiendo así ir alcanzando los objetivos parciales de la investigación.

Se destaca la posibilidad de acceder a los especialistas entrevistados y habiendo dimensionado la vasta experiencia de estos durante la investigación de campo. Cabe señalar que cada uno en su ámbito, ya sea en el alto nivel de la conducción o bien en el manejo técnico de algunos conceptos, se desenvuelven, en términos generales, en el mismo marco conceptual, lo que permitió validar la indagación documental e identificar algunos conceptos aplicados, así como hallazgos respecto a los orígenes de la Ciberdefensa en Chile.

Finalmente, el autor destaca que una debilidad del proceso de investigación o más bien de los hallazgos, fue que existe cierta incongruencia en cómo fue concebida la Ciberdefensa en Chile, respecto a la doctrina base de los Estados Unidos o España. Muchos de los conceptos son tomados de estas doctrinas, pero no existen las estructuras nacionales que sustenten todas las responsabilidades referidas a la Ciberdefensa. Por otro lado, la vigencia del desarrollo de las operaciones en el ciberespacio permite inferir ciertos efectos que la Ciberdefensa produce en un conflicto, pero el material documentado respecto a datos concretos es de difícil acceso o bien, solo sustentados en supuestos, ya que la característica de anonimato que entrega este dominio hace difícil atribuir las acciones a un sujeto y los afectados son reacios a asumir que han sido golpeados por un ataque. Lo anterior, obligó a mantener

el proceso de investigación muy apegado a la doctrina y a términos conceptuales, más que a fundamentos estadísticos, como ejemplo del obstáculo indicado.

5.2 Propuestas

Como punto de término de las conclusiones, se estima conveniente incluir algunas proposiciones dada la naturaleza de los hallazgos, pudiendo ampliarse o bien abrirse nuevas líneas de investigación como sigue:

Primero, y considerando que el origen del tema de investigación fue generado por la Dirección de Operaciones del Ejército de Chile, se estima pertinente enviar el informe a esa dirección a través del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército, con el propósito de incluir la perspectiva abordada de los temas planteados, considerar la conceptualización del problema estratégico y sacar provecho de las estructuras comparadas, en atención a las implicancias de la creación de un Comando Conjunto de Ciberdefensa .

Otra propuesta es que, a través del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército, se genere una línea de investigación respecto a las variables PEMSII-PT en el ámbito del análisis estratégico de la Ciberdefensa, puesto que la amplitud de éste permitiría desarrollar una visión mucho más amplia, pudiendo construir una base de consulta de gran valor académico y claramente operativo.

Finalmente, el autor considera conveniente remitir el informe al Batallón de Ciberdefensa del Ejército de Chile, como material de consulta y comprensión del entorno estructural de la Ciberdefensa por sobre la Institución, y cómo operan los países referentes en la materia. Esta unidad que, si bien opera en el nivel táctico de la conducción, forma parte de la asesoría para la toma de decisiones, pudiendo ser útil para la planificación y determinación de brechas de desarrollo en el área de la Ciberdefensa institucional y conjunta.

REFERENCIAS

Alford, L. (2001). *Ciberwarefare, a new doctrine and taxonomy.* Semanytic Schoolar: 11 de diciembre, 21:32 https://www.semanticscholar.org/paper/ Cyber-Warfare-%3A-A-New-Doctrine-and-Taxonomy-Alford.

Amich, C y Velasquez, A. (2014). *La Ciberdefensa y sus Dimensiones Global y Específica en la Estrategia de Seguridad Nacional Española*. Revista cuatrimestral de las Facultades de Derecho y Ciencias Económicas y Empresariales, N.º 92 mayo-agosto 2014, ISSN: 1889-7045.

Angellini, L; Maymir-ducharme, F; Stapletón, D. (2021). *Improving Decision Making by Reducing Uncertainty in Complex Systems of Systems*. NATO, Ready for the Predictable, Prepared for the Unexpected – M&S for Collective Defence in Hybrid Environments and Hybrid Conflicts. 2016.

Berkebile, R. (2018). *Una crítica a la Fórmula de Lykke.* Military Review Online.

Bloomfield, R. (2019). *Bullets to bytes: Defendig the United Kindom in Cyberspace*. Septiembre 2019, Universidad de Buckingham.

Cahanin, S. (2012). *Principles of War for Cyberspace.* Air University, Air War College. Maxwell Air forcé base, Alabama.

Cárdenas, W. (2015). *Ciberdefensa y Ciberseguridad en el sector Defensa de Colombia.* Universidad Piloto de Colombia.

CBS, News (2009). *Spies Penetrate U.S. Electrical Grid*: National Security Officials Say System Is Under Attack From Russian And Chinese Cyber Spies. April 2009. http://www.cbsnews.com

CEEAG. (2017). *Investigación en Ciencias Militares claves metodológicas.* Santiago.

Cervantes, D. (2017). *Investigación en Ciencias Militares, claves metodológicas.* Santiago, Chile: CEEAG.

Cerri, T; Sleevi N. (2016). *Simulation of Cyber Impacts on PMESII-PT Variables.* I/ITSEC. https://community.apan.org/wg/tradoc-g2/tradoc-g-27-models-and-simulations/m/documents/237949.

Colombia, FFMM. (2015). *Ministerio de Defensa de Colombia: Reseña Histórica*. Bogotá, Colombia. https://www.mindefensa.gov.co/ irju/portall/ Mindefensas/contenido? NavigationTarget=navur l://37b759d0e 31f2044d8e 555a205cf4444.

Colombia, E.N. (2015). *Comunicaciones Operacionales y Ciberdefensa.* Bogotá, Colombia.

Colombia, E.N. (2017). MFE 1-01 *Doctrina.* p:23. Bogotá, Colombia.

Colombia, CEDCO (2018). M1A 1.0 *Doctrina Conjunta.* p:25; p:57; p:241. Bogotá, Colombia.

Colombia, EST.N. (2020). *Estrategia Nacional de Ciberseguridad y Ciberdefensa de Colombia 2020-2030*. Bogotá, Colombia.

Colombia, CGFA (2022). *Organigrama del Comando General de las Fuerzas Armadas de Colombia*. https://www.cgfm.mil.co/es/conocenos /organigrama. Marzo, 2022.

Diario Oficial de Chile. (2018). “Política de Ciberdefensa”. p:1-6. Santiago, Chile.

Ejército de Chile, (2016). RDPL-20001. “Proceso de las Operaciones”. Santiago, Chile: DIVDOC.

Ejército de Chile, (2017). D-10001 “El Ejército”: p 137. Santiago, Chile: DIVDOC.

Ejército de Chile, (2018). DD-10001. “La Fuerza Terrestre”. Santiago, Chile: DIVDOC.

España, (2013). *Estrategia de Ciberseguridad Nacional.* Gobierno de España, Ministerio de Defensa de España, Madrid. 2013.

España, (2014). Ministerio de Defensa de España, *Estrategia de la Información y seguridad en el Ciberespacio.* NIPO: 083-14-062-2 (edición libro-e) ISBN: 978-84-9781-934-3 (edición libro-e).

España, (2018). Ministerio de Defensa de España, PDC-01 (A) *Doctrina para el empleo de las Fuerzas Armadas.* NIPO038-18-027-0, Madrid.

España, (2018). *Concepto de Ciberdefensa* Ministerio de Defensa de España, Estado Mayor de la Defensa. Resumen Ejecutivo. Madrid, 2018.

España, (2020). Estado Mayor de la Defensa, PDC-00 *"Glosario de terminología de uso conjunto"*. Madrid.

España, (2022). *Organigrama del Estado Mayor de la Defensa*. https://emad.defensa.gob.es/emad/estructura_cg_emad/

Esper, M. (2019). *Esper Describes DOD's Increased Cyber Offensive Strategy*. https://www.defense.gov/Explore/News/Article/Article/1966758/esper-describes-DODs-increased-cyber-offensive- strategy/.

Estados Unidos (2014). JP 2-1-3 *"Joint Intelligence Preparation of the Operational Environment".* DoD. Joint Publication. Washintong, USA.

Estados Unidos (2018). JP 3-12. *"Cyberspace Operations".* DoD. Joint Publication Washintong, USA.

Estados Unidos (2018). JP 3-0 "Joint Operations". DoD. Joint Publication. Washington, USA.

Estados Unidos, (2019). DoD. *Ciber1 Smart Book.* Washington DC: USA.

Estados Unidos (2019). *Organization and Management of the Department of Defense*. DoD. Resource Guide V3.2. Washintong DC. Marzo, 2019.

Estados Unidos, (2020). DoD JP 5-0. "*Joint Planning".* Washintong DC: USA

Estados Unidos, (2020). DoD. JPN 2-19 "*Strategy".* Washintong DC: USA

Estados Unidos, (2021). "*Dictionary of Military and Associate*". DoD Washintong DC, USA.

Farmer, D. (2010). *Do the Principles of War Apply to Cyber War.* School of Advanced Military Studies; United State Army Command and general Staff College. Fort Leavenworth, Kansas.

Finney, N. (2020). *On Strategy.* Kansas, Estados Unidos.

Gómez C; Luciano, S; Carlos, F. (2020). *Análisis y estrategia de implementación de un marco de trabajo de ciberseguridad para la unidad de Ciberdefensa del Ejército Nacional*. Universidad de Los Andes, Colombia.

Griffiths, S (2005). *El Arte de la Guerra.* Sun Tzu. Librero, edición ilustrada. Oxford University Press, reeditado.

Hernández S., R. (2014). *Metodología de la Investigación* (Vol. 6ta edición). México: Mc Graw Hill Education.

Hidalgo, J. (2013). *Principios de una conciencia nacional de ciberseguridad.* España: Ministerio de Defensa.

Autor	Fecha	Título	Fuente
Kinast, R.	(2019)	Requerimientos de Estado Mayor para el desarrollo de una Unidad de Ciberdefensa (Tesis de Estado Mayor, Academia de Guerra)	Ejército de Chile

Leiva, R. (2017). *Divisoria de Aguas entre Ciberdefensa y Ciberseguridad.* Revista de Ensayos Militares, p.3

Leonhard, R. (1991). *El Arte de la Maniobra: Guerra de Maniobra y Batalla Aeroterrestre.* Ney York, Estados Unidos: Ballantine Books.

Leonhard, R. (1998). *The Principles of war for the Information Age.* Presidio Press Book, Estados Unidos.

Lodeiro, A. (2011). *Posición en torno al concepto de Ciberguerra.* Inteligencia.

Mallik, PJ. (2020). *Principles of War, time for Re-Look.* Research Gate, Octubre 2020. https://www.researchgate.net/publication/344737409_PRINCIPLES_OF_WAR_-TIME_FOR_RE-LOOK

Masalleras, M (2021). *Seguridad y ciberseguridad: precisiones sobre una tarea compartida.* AthenaLab, Colaboración externa N.º4, Santiago de Chile.

Ministerio de Defensa Nacional (2011). DNC. "*Doctrina para la Acción Conjunta de las Fuerzas Armadas".* Santiago, Chile.

Ministerio de Defensa Nacional (2015). DNC 5 - 0. *"Doctrina Conjunta para la Planificación de Operaciones de las Fuerzas Armadas"*. Santiago, Chile.

Ministerio de Defensa Nacional (2016). DNC. *"Preparación de Inteligencia del Ambiente Operacional Conjunto (JIPOE)"*. Santiago, Chile.

Ministerio de Defensa Nacional (2017). "*Política Nacional de Ciberdefensa".* Santiago, Chile.

Ministerio de Defensa Nacional (2018). DNC 2-11. Doctrina Nacional Conjunta "*Doctrina Conjunta de Ciberdefensa".* p:14 Santiago, Chile.

Ministerio de Defensa Nacional (2022). *Organigrama de la Jefatura del Estado Mayor Conjunto*. https://www.emco.mil.cl/ index.php/ organigrama/. Marzo, 2022.

OTAN, Organización del Tratado del Atlántico Norte (2019). AJP 5 *Allied Joint Doctrine for the Planning of Operations.* Edición A, Versión 2, con elementos de la Doctrina del Reino Unido. p: 1-3

OTAN, Organización del Tratado del Atlántico Norte (2019) AJP-3 *Allied Joint Doctrine for the Conduct of Operations.* Edición C, Versión 1, Sect. N.º2

Peñaloza, P. (2017). *La Problematización Científica.* Santiago, Chile.

Reino Unido. (2017). Army Doctrine Publication *"Operations"*. p:33 Ministerio de Defensa, Londres.

Reino Unido. (2022). *Strategic Command*. UK Government Site. https://www.gov.uk/government/organisations/strategic-command.

Reino Unido. (2022). *National Cyber Strategy*. HM Government Site. Londres, 2022.

Rivas, R. (1968). *Principios de la Guerra*. Revista de Marina. Valparaíso, 1968.

Roldán, J. M. (2013). *Monografías 137 Necesidad De La Conciencia Nacional De Ciberseguridad. "La Ciberdefensa: Un Reto Prioritario".* Madrid, España: Ministerio De Defensa De España.

Royal College of Defense Studies, (2017). RCDS, U. *Getting Strategy Rigth (Enough).* P:3-8. Londres

Sánchez, G. (2009). *Internet: una herramienta para las guerras del siglo XXI.* Revista Política y Estrategia: ANEPE.

Valencia, A.; Patiño, O; Arenas, A. (2020). *Tendencias Investigativas en el estudio de Ciberdefensa: un análisis bibliométrico.* RISTI Revista Ibérica de Sistemas y Tecnologías de la Información (366-379).

Villanueva, J (2018). *La Ciberdefensa en Colombia.* Universidad Piloto de Colombia. 2018.

Wallace, W. (2008). *El Plan de Acción del Ejército.* Military Review. Julio -Agosto 2008.

Anexo 1

ENTREVISTA A ESPECIALISTAS

I. FINALIDAD

El instrumento fue estructurado para obtener información de especialistas en áreas específicas del trabajo de investigación que se realiza, tanto en aquellas referidas a la conducción estratégica como específicas en Ciberdefensa con el propósito de alcanzar los objetivos específicos planteados en el presente trabajo.

II. ESPECIALISTAS CONSIDERADOS PARA LA ENTREVISTA:

A. Profesionales de las Fuerzas Armadas (en servicio activo o condición de retiro) que tengan conocimientos especializados sobre estrategia, nivel de la conducción estratégica de Chile y que, a su vez, posean postgrados en las áreas de las Ciencias Políticas, Seguridad y Defensa.

B. Profesionales que se encuentren desempeñando docencia en Institutos de Educación Superior (grado académico de magister o doctorado) y que estén vinculados con las áreas de Ciberseguridad, Ciberdefensa y Defensa.

C. Profesionales que desempeñen funciones en el Ministerio de Defensa y/o el Estado Mayor Conjunto, vinculados con planificación estratégica y/o Ciberdefensa.

III. DESARROLLO DE LA ENTREVISTA

A. Presentación

Dar a conocer a los especialistas los motivos por los cuales se está desarrollando la presente investigación en el marco que establece el programa de estudios del Curso Regular de Estado Mayor (CREM) y cómo su aporte contribuye al proceso.

B. Introducción

Describir, en términos generales la investigación que se está realizando y enmarcar el contexto en que se desarrollará la entrevista, la cual será semiabierta, de opinión y conocimiento, lo que permite al experto referirse en un amplio sentido al tema. Se declara que la información vertida será para uso de este autor en el ámbito académico y específicamente en el desarrollo de esta investigación.

C. Preguntas asociadas al problema estratégico y la conducción estratégica

1. Conforme a la Ley 20.424 “Estatuto Orgánico del Ministerio de Defensa Nacional”, establece que la conducción estratégica de las fuerzas depende del JEMCO, quedando de manifiesto que este es el nivel de la conducción estratégica nacional, conforme a su juicio y experiencia, ¿qué características tiene el *problema militar* de este nivel?

2. Conforme al estudio del problema militar y basado en la doctrina nacional el conductor militar puede enfrentarse a problemas estructurados, semi o medianamente estructurados y mal estructurados, estableciendo que mientras más alto el nivel de la conducción mayor será la cantidad de variables y por lo tanto se tiende al enfrentamiento de un mayor número de problemas mal estructurados. ¿Por qué el problema estratégico es *per se* un problema mal estructurado? ¿cómo definiría US (Ud.) el *problema estratégico*?

3. Conforme al encuadramiento del nivel estratégico de conducción en el ámbito nacional, una metodología para la comprensión del ambiente operacional y el problema militar del JEMCO es el análisis de las variables políticas, económicas, militares sociales, infraestructura, información, espacio y tiempo (PEMSII-PT), ¿Agregaría alguna otra como aspectos legales u otros? ¿Por qué?

4. Considerando sólo las variables militares, infraestructura e información, ¿cree US (Ud.) que se puede establecer una maniobra estratégica a través de la Ciberdefensa? ¿Por qué?

5. La Política Nacional de Ciberdefensa establece que *"es la respuesta a los nuevos riesgos y amenazas que el ciberespacio le genera a la Defensa Nacional"* y, en sus diferentes artículos establece conceptos asociados a la conducción estratégica nacional e incluso a asumir la creación de un Comando Conjunto de Ciberdefensa como Argentina, Brasil, Colombia, Perú, entre los más destacados del Cono Sur, ¿por qué cree US (Ud.) que la Ciberdefensa solo ha quedado como responsabilidad de la Dirección de Inteligencia de la Defensa (DID) en el EMCO?

6. Finalmente, según su opinión y experiencia ¿cuáles son las características por las que US (Ud.) considera que la Ciberdefensa constituye un problema del nivel estratégico de la conducción, además de lo establecido en la PNCD que así lo impone?

D. Preguntas específicas Ciber Defensa

1. Producto de la revisión de bibliografía nacional y extranjera, el memorista ha establecido que el ciberespacio se entiende como: *el entorno físico y abstracto que se desenvuelve en el ambiente de la información, e involucra las plataformas, capitales de información y las relaciones e interacciones sociales que tienen lugar en este.* ¿US (Ud.) está de acuerdo con esta definición conceptual? ¿qué ajustes o modificaciones le haría?

2. En La Política Nacional de Ciberdefensa se define a esta como: *el conjunto de principios, políticas e instrumentos destinados a proteger el ciberespacio desde un punto de vista de la defensa nacional y estratégico-militar*. ¿Cuáles cree US (Ud.) que son las características de la Ciberdefensa que la determinan como objetivo estratégico-militar?

3. Conforme a la definición de Ciberdefensa de la pregunta anterior, ¿Qué opina Us., (Ud.) sobre la suficiencia de encuadrar la Ciberdefensa nacional en la DID dar respuesta a la expectativa de la Defensa Nacional en este ámbito?

4. Considerando siempre la misma definición de *Ciberdefensa* y asumiendo el empleo militar en el ciberespacio ¿Cuáles de los principios de la guerra del nivel

conjunto son aplicables? ¿cree US (Ud.) que son válidos para considerar la estructuración de una maniobra estratégica?

5. ¿Cuáles cree US (Ud.) que son los efectos positivos y negativos al considerar a la Ciberdefensa como parte de la maniobra estratégica?

Anexo 2

PROCESAMIENTO DE ENTREVISTAS

Para poder dar validez y rigor científico a la investigación, además de la revisión y comparación bibliográfica se consideró realizar entrevistas a especialistas, conforme a los perfiles declarados en el capítulo primero, siendo entrevistados los siguientes especialistas:

- Especialista N.° 1 GDD. John Griffiths Spielman.[50]
- Especialista N.° 2 GDD. Rodrigo Pino Riquelme.[51]
- Especialista N.° 3 GDD. Pedro Varela Sabando.[52]
- Especialista N.° 4 GDB. Mario Grez Casanueva.[53]
- Especialista N.º 5 CRL. Álvaro Vera Soto.[54]
- Especialista N.º 6 CRL. Fernando Meléndez Hernández.[55]
- Especialista N.° 7 CF. Roberto Siña Lazo[56]

---

50 GDD. John Griffiths Spielman, es Oficial de Estado Mayor del Ejército de Chile, fue el Jefe del Estado Mayor General del Ejército, entre los años 2017 y 2018. Posee el grado académico de Doctor en Estudios Americanos con mención en Relaciones Internacionales, en el Instituto de Estudios Avanzados de la Universidad de Santiago de Chile, entre otros estudios y grados.

51 GDD. Rodrigo Pino Riquelme, Oficial de Ejército, la especialidad primaria de Estado Mayor, especialista en Inteligencia e integrante del Comité Estratégico del Ejército. Actualmente se desempeña como Comandante de Educación y Doctrina del Ejército. Posee el grado académico de Magister en Educación en Docencia, además es Magister en Cs. Militares con mención en planificación Estratégica.

52 GDD. Pedro Varela Sabando, Oficial de Ejército, la especialidad primaria de Estado Mayor, especialista en Inteligencia e integrante del Comité Estratégico del Ejército. Jefe del proyecto de creación del Regimiento de Inteligencia N.º2 “Llaitún”, unidad responsable de la Ciberdefensa institucional. Integrante del Comité Estratégico del Ejército. Actualmente se desempeña como el Comandante de Operaciones Especiales del Ejército y posee el grado académico de Magister Cs. Militares con mención en planificación Estratégica.

53 GDB. Mario Grez Casanueva, Oficial de Ejército, posee la especialidad primaria de Estado Mayor, especialista en Inteligencia. Se desempeñó como Director de Planificación de Informaciones del Ejército (DIPLINE) y actualmente es el Comandante de la Brigada de Inteligencia del Ejército (BINTE). Posee el grado académico de Magister en Ingeniería en Sistemas Logísticos.

54 CRL. Álvaro Vera Soto, Oficial de Ejército, la especialidad primaria de Ingeniero Politécnico Militar con mención en Sistemas de Armas Electrónica, posee el grado académico de Magister en Ciencias de la Ingeniería mención Sistemas Optrónicos y Magister en Análisis de Inteligencia Comunicacional.

55 CRL. Fernando Meléndez Hernández, Oficial de Ejército, la especialidad primaria de Estado Mayor. Especialista en Inteligencia, Actualmente se desempeña como el Jefe de Ciberdefensa en el Estado Mayor Conjunto. Posee el grado académico de Magister en Ciencias Militares, con mención en Planificación y Conducción Militar.

56 CF. Roberto Siña Lazo. Oficial de la Armada de Chile, actualmente es el Jefe del Centro de Respuesta de Incidentes Informáticos del EMCO. Integrante del Proyecto “Marciano”, proyecto de implementación de Ciberdefensa en la Dirección de Inteligencia de la Defensa.

- Especialista N.° 8 TCL. Jorge Villarroel Rivera[57]
- Especialista N.º 9 CRL (COL). Harold Burbano Goyes.[58]
- Especialista N.° 10 Sr. (PhD) Gonzalo Díaz de Valdés Olavarrieta[59]

Los cuales a través de sus conocimientos en la materia presentaron diferentes posturas las que se exhiben en la tabla resumen que a continuación se presenta. Cabe destacar que por el puesto que ocupan algunos de ellos, así como por la realidad de la Ciberdefensa a nivel nacional, no fue posible transcribir la totalidad de las conversaciones, así como otros solo permitieron apuntes escritos en beneficio de la confidencialidad de los datos tratados:

Tabla "Contenidos entrevistas a expertos"

Objeto de la pregunta	Especialista	Información obtenida
Características del problema militar en el nivel estratégico	GDD. GRIFFITHS	"no estoy de acuerdo con que se plantee que el problema está mal estructurado, la estructura del problema es la responsabilidad del OEM… estoy de acuerdo que a mayor el nivel de la conducción son el mayor número de variables, es más complejo sin duda. Esta complejidad está dada por la capacidad de consecución del objetivo, con un nivel de incertidumbre alto" (2:00)
	GDD. PINO	Cómo dar respuesta al requerimiento desde el escalón político (respecto a la Defensa nacional) (2:00). El nivel de complejidad o estructuración dependerá de lo que necesita el poder político. Es multi factorial (3:25)
	GDD. VARELA	El gran problema de este nivel es que sobrepasan el accionar militar, lo que requiere un profundo análisis del ambiente estratégico, considerando que la opción de respuesta militar que va a ser contribuyente a otros elementos del poder natural. (1:35) Es un problema mal estructurado, por la gran cantidad de variables que lo afectan, y por más que se analice todo, no se asegura el éxito de solución, se pude acortar la brecha sin

[57] TCL. Jorge Villarroel Rivera, Oficial de Ejército, posee la especialidad primaria de Estado Mayor, Profesor Militar de Academia en la asignatura de Inteligencia, posee el grado académico de Magister en Educación con mención en Docencia de Nivel Superior. Actualmente se desempeña como Comandante del Batallón de Ciberdefensa del Ejército.

[58] CRL. Harold Burbano Goyes es Oficial de Estado Mayor del Ejército de Colombia, especialista en Inteligencia y Subjefe de la Unidad de Inteligencia Operativa del Ejército Nacional. Profesor Invitado en la Academia de Guerra del Ejército de Chile, adjunto al Departamento de Operaciones Militares.

[59] SR. Gonzalo Diaz de Valdés Olavarrieta, es asesor del Ministerio de Defensa Nacional en materias de Ciberseguridad, posee el grado académico de Doctor en Sistemas de Ingeniería Civil de la Universidad Politécnica de Madrid y MBA de la Universidad de Maryland, Estados Unidos.

Objeto de la pregunta	Especialista	Información obtenida
		duda, pero eso es lo complejo. (2:34). Un ejemplo claro es la salida abrupta de USA de Afganistán.
	GDB. GREZ	Siempre enmarcado en el tema de la Ciberdefensa, el problema estratégico está afectado por múltiples variables, donde los límites entre un nivel y otro son difusos, esa condición de incertidumbre lo hace complejo y si además sumamos que no es estático más complejo aún.
	CRL. VERA	Desde mi punto de vista, es complejo y está afectado por muchas variables, pero principalmente lo veo por el desarrollo de capacidades para poder dar satisfacción al nivel de esfuerzo exigido a la fuerza en el contexto de los objetivos políticos de la Nación.
	CF SIÑA	Es complejo, tiene demasiadas variables, aspectos legales que limitan más que permiten, normalmente la planificación estratégica para alcanzar los objetivos va asociada a desarrollo de capacidades para poder cubrir brechas y cumplir objetivos realistas, se debe buscar un equilibrio entre el objetivo y lo que soy capaz de hacer. Además de tener que articular el idioma entre las mismas instituciones.
	TCL. VILLARROREL	el problema se vuelve mucho más complejo y mal estructurado que en los niveles inferiores de la conducción militar. Este conductor militar tiene injerencia en todos los dominios (terrestre, marítimo, aéreo, espacial y del ciberespacio) y en el que operan capacidades militares muy disímiles entre sí. Además de que el contexto actual impone hacer frente a diferentes áreas de misión y ejecutar Operaciones Militares de guerra y distintas a la guerra. Finalmente, el conductor militar en este nivel interactúa con actores de distintas funciones, ámbitos y sectores.
	CRL. BURBANO	- Mantener la capacidad necesaria para neutralizar amenazas internas, externas o hibridas - Proyectar el ejército del futuro, con menos recursos, pero con más exigencias y más amenazas. - La formación de líderes multi-misión, capaces de enfrentar ambientes VICA (volátiles, inciertos complejos y ambiguos) que encajen en equipos de trabajo modulares de acuerdo a la misión a desarrollar.
	SR. DIAZ DE V.	Es un entorno hostil, complejo e interconectado (10:41) con entornos híbridos con “armas cibernéticas” con capacidad de destrucción de sus capitales de información para afectar la toma de decisiones. (11:29).
¿cómo definiría el problema estratégico?	GDD. GRIFFITHS	Es un problema de múltiples variables, es necesario entender la esencia del nivel estratégico y entender que la fuerza militar se emplea en un ambiente de fricción. Ese contexto del nivel

Objeto de la pregunta	Especialista	Información obtenida
		estratégico tiene componentes de complejidad y de alta incertidumbre. Aplican para este nivel los escenarios VUCA más lo disruptivo.
	GDD. PINO	Es un problema multifactorial, múltiples variables. Está de acuerdo con la definición establecida por el autor.
	GDD. VARELA	Conforme a nuestra doctrina, es aquel del ámbito del JEMCO y que debe articular los medios de la Defensa Nacional, proponer los modos para poder dar cumplimiento a los fines del escalón político.
	GDB. GREZ	En la realidad nacional, como un problema que debe articular el empleo del poder militar para alcanzar los objetivos del poder político.
	CRL. VERA	Problema de la alta dirección y toma de decisiones que debe buscar contar con las capacidades necesarias para dar respuesta a los objetivos que se le plantean.
	TCL. VILLARROEL	Es más complejo, debido a que son múltiples las variables que impactan en el problema, difíciles de integrar, en el que puede presentarse un alto volumen de información, con carencia de herramientas de procesamiento de datos y con tiempos limitados. Por otra parte, son problemas de una estructura sin una solución única, simple o que permita asegurar que este sea resuelto, pudiendo hacer frente con COAs diversos y variados. Por lo anterior, **podría aseverarse que el problema estratégico es complejo y mal estructurado.**
	CRL. BURBANO	Su resolución no tiene una formula militar por sí sola, requiere de la integración de esfuerzos, agencias y recursos, acompañada de una decisiva voluntad política. La repetición de resultados táctico-operacionales contribuyen a un logro estratégico.
	SR. DIAZ DE V.	Como una situación que posee una superficie de exposición a las naciones y los estados cada vez mayor (08:32), se dan condiciones que relacionadas entre sí son muchas más complejas y sinérgicas. Que actualmente las capacidades de influencia en el ciberespacio son inconmensurables, por lo que el problema de este nivel no tiene solución predecible.
¿Otra variables además de PEMSII-PT?	GDD. GRIFFITHS	"variables culturales y sociales, idiosincrasia, sin duda la variable legal es clave, el OEM debe ser formado en forma integral, necesidad de entender el contexto ene l que se usa la fuerza" (4:30) "Las variables, no son dogma de fe, se deben incorporar todas las variables necesarias"
	GDD. PINO	Sin duda hay que mantener siempre presente el tema legal, hoy en día no se puede dejar de lado (20:19), no solo es

Objeto de la pregunta	Especialista	Información obtenida
		necesaria, es hasta innovadora en el ámbito de la ciber defensa.
	GDD.VARELA	No olvidar que PEMSII viene de la doctrina OTAN, por lo que hay que entender que la doctrina hay que adaptarla a diferentes metodologías de análisis. Pero es eso una metodología. (4:40). La generación del JEMCO permite adaptar estas metodologías, pero finalmente la conclusión es que hay que agregar los factores necesarios para dar un buen entendimiento del ambiente. (05:54) El mundo de la Ciberdefensa hoy marca un cambio tan radical como el uso del espacio aéreo el siglo pasado (6:49), hay que entender que la ciber no responde ni a fronteras ni a leyes y las leyes que existen van asociadas a delitos (7:32). Este escenario es anárquico, y hay que poder operar en él.
	GDB. GREZ	No hay que perder de vista que las variables PEMSII son una herramienta de varias más que existen, si bien la doctrina nacional propone esta herramienta de análisis no hay que olvidar que la doctrina es una guía, por lo que hay variables como las legales, culturales, coyunturales de cada problema. Me inclino por decir que las variables PEMSII son la base y deben ser complementadas por lo legal y todo aquello que, considerando el tiempo disponible, aporte a una comprensión del problema y a la toma de decisiones.
	CRL. VERA	Creo que variables son múltiples y además que si la doctrina sugiere esa metodología no es una caja cerrada, es decir, la doctrina sugiere el desde. Yo le agregaría aspectos sociales y legales. Como lo que estamos viendo hoy en Ucrania.
	CRL. MELENDEZ	La variable legal debe ser considerada, el Manual de Tallin para las naciones de la OTAN es una muestra de ello, no se puede omitir en ningún caso este aspecto a pesar de que exista la capacidad de repudiar un ataque.
	CF. SIÑA	Creo que desde el punto de vista de la Ciber, es el desde la metodología PEMSII, hoy que agregar toda aquella que pueda afectar en sus efectos al Estado, lo que sean necesario. Lo legal por supuesto, lo social, la infraestructura crítica, lo importante es que esto sea centralizado en la planificación del EMCO y no cada uno por su lado.

Objeto de la pregunta	Especialista	Información obtenida
	TCL. VILLARROEL	Para comprender el ambiente operacional, los factores de análisis son más amplios y variables, excediendo en muchas oportunidades a los comúnmente estudiados PMESII-PT, pudiendo efectivamente integrar aspectos legales, o, como menciona la doctrina de Inteligencia de Naciones Unidas, factores Culturales, Históricos y Religiosos (PMERSCHIIPT) y eventualmente otros (como en el caso del despliegue de capacidades en apoyo al EEC-C por la Pandemia, la inclusión de un factor sanitario). En este sentido, es relevante que un conductor militar expuesto a problemas complejos y mal estructurados debe tener la capacidad de integrar todas las variables posibles (en el tiempo disponible) y no limitarse exclusivamente conocido.
Factibilidad estructurar la maniobra estratégica a través de la Ciberdefensa	GDD GRIFFITHS	"indudablemente y esta debe ser incluida desde tiempo de paz, sobre todo un empleo asimétrico de la fuerza" (06:40) *Este dominio permite volver a recordar a Sun Tzu, y lograr ganar la guerra sin disparar un tiro.* *"Es una herramienta estratégica, que genera condiciones (configura) para lograr los objetivos estratégicos, operacionales o tácticos.*
	GDD PINO	Claro que puede y específicamente es la gran configuración de la maniobra estratégica terrestre. (24:06)
	GDD VARELA	Creo que incluso pude ser una maniobra estratégica independiente (14:22). Se pueden alcanzar objetivos políticos con la gran capacidad de lograr efectos físicos y sicológicos. Si lo estructuramos en fines, medios y modos. Pero a tu pregunta puede colaborar o ser una maniobra per se (15:22)
	GDB GREZ	Si, creo que hoy la Ciberdefensa permite preparar o condicionar escenarios con las capacidades del poder militar, en favor de una maniobra del Estado, especialmente desde mucho antes del empleo del potencial bélico. Las capacidades de la Ciberdefensa para influir en el ambiente de la información sin afectar la dimensión física pueden condicionar la toma de decisiones del adversario.
	CRL. VERA	No sé si en base a la Ciberdefensa, pero si concuerdo en que hoy no se puede dejar de lado y debiera ser la primera opción de respuesta ya que con pocos medios se puede trabajar desde antes del empleo del potencial bélico.
	CRL MELENDEZ	Por supuesto, y hasta político estratégico, es cosa de ver el ejemplo de RUS-UCR que antes de iniciar las grandes ofensivas, durante semanas se hizo una maniobra de configuración estratégica a través de ciberoperaciones.
	CF. SIÑA	Absolutamente y me tomo de las palabras del General Iturriaga, desde el EMCO lo fundamental será la planificación

Objeto de la pregunta	Especialista	Información obtenida
		y coordinación de la maniobra, para que la ejecución y conducción sean descentralizadas.
	TCL VILLARROEL	No, ya que una Ciberoperación para este nivel de la conducción, obedece a la solución a un problema de ese nivel, que necesariamente analizó el máximo de variables (y factores) que deben, al menos, incluir otros aspectos; como el espacio físico (y del ciberespacio), el tiempo disponible, factores legales y sociales. - Físico, ya que una capa para el estudio del ciberespacio es física, donde se almacena y se ubican componentes informáticos, lo que puede afectarse con capacidades de Ciberdefensa o con la acción de otras capacidades militares variadas (Fuegos Letales y no letales, Operaciones Especiales, HUMINT, entre muchas otras). - Tiempo disponible, ya que una ciberoperación requiere de una cadena de acciones para alcanzar un objetivos (ver etapas de CyberKillChain). - Legal, debido a que el empleo para el empleo ofensivo (COps-O) tiene un enfoque de Fuegos No Letales (asociados al Proceso de Targeting que tiene una participación de un asesor legal) o de Inteligencia (inteligencia o contrainteligencia), que deben ser pertinentes a la Ley de Inteligencia. - Sociales, debido a que una de las principales vulnerabilidades de los sistemas informáticos es la capa humana, por lo que la aproximación con ingeniería social es relevante.
	CRL. BURBANO	Si, Tiene el objetivo de detectar las amenazas y vulnerabilidades a los cuales se exponen las operaciones en el ciberespacio y dar una eficiente respuesta, en tiempo real, para desarticular las ciberamenazas. El ciberespacio se convierte en un nuevo campo de acción que contribuye de forma decisiva para el desarrollo de operaciones. Es un escenario novedoso de cooperación y desarrollo, pero, así mismo, de riesgo. Por tanto, se debe estar preparados para proteger su infraestructura, sus centros de mando y control y todas las acciones que de una o de otra forma protegen la seguridad de la fuerza
	SR. DIAZ DE V.	Sin duda, hoy es inconcebible plantearse una acción en el ámbito de la respuesta militar que no considere acciones defensivas, protección de sistemas tecnológicos y ofensivas a través de las ciberoperaciones.
Pertinencia del encuadramiento	GDD. GRIFFITHS	"…no es pertinente, a mi juicio pasa por una parte debido a la ignorancia respecto a entender una nueva dimensión, por lo

Objeto de la pregunta	Especialista	Información obtenida
de la Ciberdefensa en la DID		que se encuadra en algo conocido… pero no es algo de inteligencia…. luego a la coyuntura legal nacional, por el amparo de la Ley de Inteligencia" (11:00)
	GDD. PINO	El encuadramiento de la ciber en la DID es para darle un "paraguas" bajo el amparo de la Ley de Inteligencia. Tiene un sustento para poder realizar operaciones de las características que realiza. Le da una legitimidad no ilimitada (35:32)
	GDD. VARELA	Tiene que ver por una situación coyuntural política por la estructura nacional. Hoy hay una deficiencia en la regulación de la IC del ámbito militar y privado. La creación de un CC no es tan urgente como la gobernanza respecto a responsabilidades y definición de IC. (11:30) Gracias a la protección de la Ley de Inteligencia, se le enmarca ahí para estar al amparo. (12:44) Opino que es tan relevante la ciber que debiera ser independiente.
	GDB. GREZ	Creo que para dar respuesta al requerimiento de la Política Nacional de Ciberdefensa el año 2018 fue pertinente, ya que permitió trabajar al amparo de la Ley de Inteligencia, refuerzo que estoy de acuerdo con el momento que se vivía y estar bajo la ley permitía hacer operaciones intrusivas y contar con financiamiento para el desarrollo de capacidades. Por otro lado, la Ciberdefensa ha crecido al amparo de la inteligencia, pero sin duda sus alcances exceden a la amplitud de las operaciones de inteligencia y tiene concordancia con la necesidad de crear un Comando Conjunto, que reúna las capacidades para la coordinación de ciber operaciones y ciber inteligencia conforme a los requerimientos del poder político
	CRL. VERA	Creo que era necesario en un principio, y fue consecuencia de otras cosas debido a que la asociaron como a capacidades de Guerra Electrónica, de ahí deriva el traspaso de la EW a inteligencia para quedar al amparo de la ley y en consecuencia la Ciberdefensa quedó ahí. Para el momento en que se vivía si fue pertinente, con los antecedentes y evolución abiertamente debe ser independiente de la inteligencia, pero siempre en el EMCO, así coordinar los esfuerzos.
	CRL. MELENDEZ	Obedece principalmente por el amparo de la Ley de Inteligencia que es una ley de quorum calificado, esto debido a que todas las acciones de intrusión solo pueden estar avaladas por esta ley, por tanto, la única opción fue encuadrarlo acá e incluso al día de hoy se ha dejado al DID como el futuro comandante de Ciberoperaciones, a mi juicio un error, pero así está concebido.

Objeto de la pregunta	Especialista	Información obtenida
	CF. SIÑA	A la luz de lo que vivimos hoy no es pertinente ya que sabemos que la función es mucho más allá de la exploración y solo la asesoría para la toma de decisiones, pero hay que entender el pasado y como se genera esto a partir del 2012 con algunos proyectos de las FAs, la protección de señales, la Guerra electrónica, etc. Las instituciones fueron desarrollando algunas capacidades de este tipo como contra inteligencia, eso sumado a las facultades de la Ley de Inteligencia y como esto aportaba desde el punto de vista del presupuesto para el desarrollo de capacidades llevó a que se centralizar en un proceso bottom up, es decir desde las instituciones hacia arriba. Lo importante hoy, no creo que sea que esté en la DID, si es importante que esté en el EMCO y progresando en este nivel. Eso lleva solo a concluir que es necesaria la centralización de la planificación en el nivel estratégico.
	SR. DIAZ DE V.	Fue por un tema de conocimiento y comprensión de tecnologías de información avanzada (15:50) cuando se crea la estructura de Ciberdefensa, las direcciones de inteligencia fueron las más avanzadas en esas materias y se podía construir desde una base. Aun cuando no son necesariamente pertinentes hoy, pero se partía de una base consistente. (17:10). Creo que lo de la DID es irrelevante, lo importante es que se haya generado en el EMCO como el gran coordinador y conductor estratégico, esa es la mirada que debemos dar.
	TCL. VILLARROEL	El EMCO se encuentra en el proceso de estudio para la creación del Comando Conjunto de Ciberdefensa en un horizonte de mediano plazo. No obstante, la Ciberdefensa ha mantenido su vinculación a la Inteligencia, por haber evolucionado desde la Seguridad Computacional a la Seguridad Informática y actualmente al rol de una capacidad militar que se incrementa gradualmente (actualmente el EMCO tiene un CSIRT y el Centro de Coordinación de CSIRT Defensa). Tal como otras capacidades (como EW y Exploración), se estableció que depende de la Inteligencia Militar, ya que, en sus empleos, mantiene 3 roles fundamentales; - Inteligencia (una capacidad de obtención de información). - Ofensivo (como capacidad que se mantiene asociada a una OEI). En este ámbito, cobran relevancia dos aspectos; - Que la creación del EMCO en 2010 (Ley 20.424), se explicita que el Conductor Estratégico recibe las Fuerzas de Tierra, Aire y Mar para la Crisis y EPB. No obstante, esto no obedece a las Instituciones (Ejército, Armada y Fuerza Aérea) o los Dominios (Terrestre, Marítimo, Aéreo, Espacial y Ciberespacio),

Objeto de la pregunta	Especialista	Información obtenida
		quedando un vacío en el que no se menciona la Ciberdefensa en particular, que podría constituirse como una oportunidad para definir si el EMCO poseerá una Capacidad "ejecutiva" y "permanente" de Ciberdefensa. - En primer término, la relación de un organismo de carácter "directivo" como la DID, puede tener pertinencia sobre la Seguridad de Sistemas Informáticos y algún requerimiento de Inteligencia que pueda solicitarse a las Instituciones (ya que las instituciones tienen las facultades para la ejecución de operaciones de inteligencia). No obstante, considerando la respuesta A.5., la función de Operaciones debe asumir un rol ante el empleo de capacidades de Ciberdefensa como fuegos no letales. - En cuanto al rol ejecutivo, tanto la DID, como el EMCO en su conjunto, no tienen capacidades ejecutivas permanentes, a excepción de lo establecido en la Ley 20.424, por lo que las capacidades de Ciberdefensa se han mantenido en las Instituciones. Existiendo una oportunidad por los vacíos que presenta esta Ley, relativos al ciberespacio. Sin perjuicio de lo anterior y observando la experiencia de otros países, de contar con una capacidad ejecutiva y permanente de Ciberdefensa en el EMCO (Comando Conjunto de Ciberdefensa), es recomendable mantener capacidades en las Instituciones.
Las características de la Ciberdefensa son suficientes para ser consideradas como un problema estratégico-militar	GDD. GRIFFITHS	Absolutamente, es una dimensión que debe ser y será explotada por las componentes militares con las capacidades instaladas en pos del objetivo político entregado.
	GDD. PINO	Si son suficientes, especialmente por los impactos que tienen o pueden tener sus acciones (36:32). Además, por la capacidad de afectar otros actores y otros intereses que comprometan aún más una opción de respuesta militar (41:04).
	GDD VARELA	Es un problema político estratégico, del más alto nivel (13:00), debido a los impactos y efectos en otros elementos del poder nacional.
	GDB. GREZ	Claro que sí, las capacidades de afectar tanto el ambiente de la información, como acciones físicas deben ser consideradas estratégicas especialmente basado en los efectos que estas acciones tienen. Abiertamente la Ciberdefensa puede afectar la toma de decisiones al más alto nivel al punto de disuadir o deslegitimar una postura contrapuesta a los intereses propios.
	CRL. VERA	De todas maneras, creo incluso que aún no dimensionamos los efectos que se pueden causar en forma encubierta, quién domine este ámbito puede definir el conflicto sin disparar un tiro.

Objeto de la pregunta	Especialista	Información obtenida
	CRL. MELENDEZ	Creo que con todo lo que hemos hablado, puedo decir que a pesar de que el deber ser no se cumple, por definición o por concepción si lo es.
	CF SIÑA	Creo que desde muy temprano se entendió esto desde las instituciones, hasta que se asume que debe ser planificado y coordinadas en el nivel estratégico.
	TCL. VILLARROEL	Porque proviene desde la Política de Ciberseguridad, que persigue alcanzar una condición de Seguridad en el Ciberespacio (tiene relación con el concepto de Seguridad Nacional), para lo que la Ciberdefensa representa el aporte del sector Defensa para tal objeto (condición de seguridad en el ciberespacio). Por esto, y considerando la cantidad de amenazas externas que pueden impactar esta condición de seguridad, la Defensa Nacional (particularmente la Ciberdefensa), puede asumir un rol protagónico para proteger los activos, redes, sistemas, información, etc, del país. Enfocándose especialmente en la Infraestructura Crítica de Información (ICI). Este es un aspecto aún no profundizado, ya que las instituciones aún se encuentran en proceso de desarrollo de sus capacidades de Ciberdefensa en todo su espectro (seguridad de sistemas informáticos, Ciberinteligencia y capacidades para su empleo como fuegos no letales), que las ha llevado a centrarse en su propia ICI y no en la nacional. Pudiendo ser un desafío en el mediano plazo. En este sentido, este es un problema del nivel estratégico de la conducción militar.
	CRL. BURBANO	Enfrentar los problemas y retos de conexión a las tecnologías de la información y las comunicaciones está determinada por estos dos términos (Ciberdefensa y Ciberseguridad) con los cuales se han planteado alternativas metodológicas, políticas, normas y procedimientos. De esta manera se define la Ciberdefensa como la capacidad del Estado para prevenir y contrarrestar toda la amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional Las acciones de Ciberdefensa buscan la protección en los siguientes aspectos: □ Uso de Internet con fines terroristas □ Actos de guerra cibernética □ Hechos afines con objetivos de guerra □ Espionaje La ciberseguridad es la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos ante amenazas o incidentes de naturaleza cibernética.

Objeto de la pregunta	Especialista	Información obtenida
		Las acciones de ciberseguridad buscan la protección de los siguientes aspectos: Transacciones financieras Información privada Derechos fundamentales Propiedad intelectual. Normal funcionamiento administrativo **Infraestructura crítica.** Es el conjunto de computadores, sistemas computacionales, redes de telecomunicaciones, datos e información, cuya destrucción o interferencia puede debilitar o impactar la seguridad de la economía, política, salud pública, militar o la combinación de ellas en una nación. Proyección sobre las capacidades a emplear para lograr un mejor resultado frente a una amenaza. Mantener la iniciativa prospectiva. Es el escenario donde se mueve actualmente el mundo, capacitación permanente en tecnologías. Escenario novedoso, de cooperación internacional, pero al mismo tiempo de alto riesgo. Es un factor de crecimiento no solo para la fuerza sino para toda la nación. Solucionar problemáticas en los más variados campos, impulsa la innovación. Nacimiento de nuevas amenazas Se debe tener en cuenta que con el advenimiento del ciberespacio también nacen nuevas formas de hacer la guerra, nuevos teatros de operaciones y nuevas formas de operar. Personas éticamente mal preparadas, se constituyen en alto riesgo de seguridad nacional. Lo novedoso de los fenómenos denominados como “amenazas”, es que debido a las bondades del ciberespacio se convirtieron en amenazas transnacionales asumiendo una magnitud y un alcance que trasciende las previsiones y pautas con que tradicionalmente se enfocaban las cuestiones de seguridad interior, defensa nacional y seguridad internacional. No es posible comprenderlas sin considerar la existencia de otros actores conexos.
	SR. DIAZ DE V.	Respecto a todo lo conversado con anterioridad y la necesidad de mantener la Ciberdefensa en el EMCO, es el mejor indicador que el entorno de la Ciberdefensa es un problema militar estratégico.

Objeto de la pregunta	Especialista	Información obtenida
Está de acuerdo con esta definición de ciberespacio: *"el entorno físico y abstracto que se desenvuelve en el ambiente de la información, e involucra las plataformas, capitales de información y las relaciones e interacciones sociales que tienen lugar en este"*	GDD. GRIFFITHS	"sí, estoy de acuerdo. Es posible visualizar los aspectos físicos y abstractos. No veo que la definición tenga errores conceptuales, no hay problema de lógica y coherencia" (18:00) *El ciberespacio es la único dominio de la guerra creado por el hombre y es continuo y transversal.*
	GDD VARELA	Si, estoy de acuerdo.
	GDB GREZ	Si estoy de acuerdo, aun cuando yo haría cambios desde el punto de vista del énfasis en algunas partes de la definición, pero sí considera los aspectos genéricos de lo que entendemos por ciberespacio.
	CRL. VERA	Si, estoy de acuerdo, engloba en forma genérica todos los conceptos.
	CRL MELENDEZ	Si, no le veo nada malo.
	CF SIÑA	Si estoy de acuerdo, es más cuando yo estaba acá el 2018 para la publicación de la DNC de Ciber, el concepto que se determinó vino bastante técnico, ya que a pesar de haber sido consensuado por todos, fue la FACH que tomó protagonismo con eso porque lo venían trabajando de mucho antes.
	TCL. VILLARROEL	Se recomienda tener presente lo definido en la Político de Ciberdefensa de Chile de 2018 y en la de Defensa Nacional de 2020. La definición contemplada para la actualización del RDI-20008 "Ciberdefensa", edición 2022 es "El ciberespacio (CE) es un conjunto de infraestructuras físicas, lógicas y las interacciones que ahí se producen (Político de Ciberdefensa de Chile, 2018) para el intercambio y procesamiento de información (política de Defensa Nacional de Chile, 2020). Se ha constituido como un dominio más, junto al terrestre, marítimo, aéreo y espacial, que se diferencia por ser artificial, intangible y global".
	CRL. BURBANO	Si, creo que no deja nada de lado. Mientras más genérica sea mejor permite adecuar su evolución.
	SR. DIAZ DE V.	Hay muchas definiciones, esta tiene elementos contundentes, destaco lo de las relaciones sociales que mencionas.
Aplicabilidad de los Principios de la Guerra Conjuntos para la estructuración de la maniobra de Ciberdefensa	GGD. GRIFFITHS	"La guerra no ha cambiado en su naturaleza, pero si en su carácter, por lo que creo que se deben volver a revisar los principios de la guerra para esta dimensión, porque los principios de la guerra han sido levantados sobre las tres dimensiones, no quiere decir que no sirven, por el contrario son aplicables algunos y sin duda aparecerán otros en la medida que se adquieran experiencias de su empleo" (23:43)
	GDD PINO	Los principios son una guía y creo que donde operan fuerzas militares independiente de su categoría se pueden utilizar los

Objeto de la pregunta	Especialista	Información obtenida
		principios en forma genérica, tal vez con esta dimensión hay que ajustar algunos, pero la respuesta final es si.
	GDD VARELA	Como son principios son referenciales, y dan criterios de éxito, y como son genéricos aplican, tal vez no todos, pero lo más importante es que se pueden crear nuevos conforme a las características de la ciber (17:10)
	GDB. GREZ	Todos, creo que este dominio y en concordancia con la aplicabilidad a la maniobra estratégica, los principios de la guerra son aplicables y no descarto que puedan aplicarse cosas nuevas desde el punto de vista de la temporalidad. Lo más discutible puede ser la mantención del terreno, pero si lo piensas también se debe contar con un dominio de las redes y nunca perder de vista la dimensión física del ciberespacio.
	CRL VERA	Son aplicables, creo que hay que tenerlos presentes, pero también en este ámbito hay que dejar de lado los límites espaciales y la concentración de fuerzas a veces se pierde, lo dejaría como concentración de esfuerzos.
	CRL. MELENDEZ	Son aplicables, la mejor explicación es que son un principio de optimización, son principios generales para tener en cuenta para concebir la maniobra ciber. De tal manera de asegurar una maniobra optimizada, no es dogma es una guía para acercarse a lo óptimo
	CF SIÑA	Claramente, si o si debe incluirse la metodología de planificación bajo los principios de la guerra conjuntos.
	TCL. VILLARROEL	Los principios de la guerra son totalmente validos y aplicables para toda Operación Militar de Guerra, tanto para el empleo de la capacidad de Ciberdefensa como parte de una maniobra conjunta (que integre distintas capacidades), como en una Operación exclusiva de Ciberdefensa.
	CRL. BURBANO	Si, son aplicables en especial: Flexibilidad, oportunidad, iniciativa, disuasión, economía de fuerzas.

Fuente: Elaboración propia del autor.