Capítulo 3

Capacidades del Estado colombiano para combatir las amenazas y los desafíos multidimensionales en los dominios aéreo y ciberespacial*

DOI: https://doi.org/10.25062/9786287602106.03

Iván Harvey Mora Gámez
Fabio Baquero Valdés
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo tiene por objeto establecer el impacto que generan las nuevas amenazas y desafíos multidimensionales en el interés nacional del Estado colombiano, en los dominios aéreo y ciberespacial. En primer lugar, se presenta una descripción de las nuevas amenazas para comprender su relación con el interés nacional. Igualmente, se categorizan las amenazas multidimensionales, para establecer los efectos de dichas amenazas en los ambientes aéreo, ciberespacial y multidominio. Acto seguido, se describe la forma como las amenazas multidimensionales se materializan y afectan al Estado en los dominios aéreo, ciberespacial y multidominio, e impacto sobre el interés nacional. Finalmente, se plantean las capacidades que el Estado colombiano debe desarrollar para contener y combatir las amenazas multidimensionales en los ambientes aéreo, ciberespacial y multidominio para proteger el interés nacional.

Palabras clave: Amenazas y desafíos multidimensionales, dominio aéreo, dominio ciberespacial, intereses nacionales, multidominio.

* Capítulo de libro resultado de los proyectos de investigación: 1) *Proyección del Poder Aéreo, Espacial y Ciberespacial frente a las amenazas y desafíos multidimensionales que afectan al Estado colombiano*, del grupo de investigación Masa Crítica, de la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), categorizado como A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias) y registrado con el código COL0123247; y 2) *Desafíos y nuevos escenarios de la seguridad multidimensional a nivel nacional, regional y hemisférico en el decenio 2015 - 2025*, del grupo de investigación Centro de Gravedad, de la ESDEG, categorizado como A por (MinCiencias) y registrado con el código COL0104976. Los puntos de vista pertenecen a los autores, y no necesariamente reflejan el pensamiento de las instituciones participantes.

Iván Harvey Mora Gámez
Teniente Coronel de la Fuerza Aérea Colombiana, del Cuerpo de Seguridad y Defensa de Bases Aéreas. Administrador aeronáutico, Magister en Ciencias Militares Aeronáuticas de la Escuela de Posgrados de la Fuerza Aérea Colombiana. Magister en Ciberseguridad y Ciberdefensa de la ESDEG. Contacto: ivan.mora@fac.mil.co

Fabio Baquero Valdés
Coronel de la Reserva Activa de la Fuerza Aérea Colombiana. Administrador Aeronáutico, Magister en Eduación de la Universidad Santo Tomás. Docente ocasional asociado e investigador Junior Minciencias del Grupo "Masa Crítica" en la Escuela Superior de Guerra "General Rafael Reyes Prieto" ESDEG. ORCID: https://orcid.org/0000-0002-5509-322X - Contacto: fabio.baquero@esdeg.edu.co

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

Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano
ISBN impreso: 978-628-7602-09-0
ISBN digital: 978-628-7602-10-6
DOI: https://doi.org/10.25062/9786287602106

Colección Estrategia, Geopolítica y Cultura
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes Prieto"
Bogotá D.C., Colombia
2022

Introducción

La *seguridad multidimensional* es un enfoque adoptado por la Organización de los Estados Americanos (OEA) durante la declaración de Bridgetown, en 2002, como una estrategia para abordar la seguridad. Este concepto contempla las amenazas tradicionales a la seguridad hemisférica como las nuevas amenazas que pueden enfrentar los Estados miembros de la organización (Organización de Estados Americanos [OEA], s.f.). Las nuevas amenazas se caracterizan por ser trasnacionales, y generadas, en algunos casos, por actores y organizaciones no estatales, que afectan la seguridad de uno o más Estados y, por lo tanto, dificultan la forma como se las contiene o se las combate. Por tal razón, el Estado colombiano, como miembro de la OEA, adopta el enfoque de seguridad multidimensional identificando nuevas amenazas y generando estrategias de seguridad, de modo que ello le permita emplear sus propias capacidades para enfrentarlas y visualizar los nuevos desafíos que se puedan presentar.

Ahora bien, las nuevas amenazas que afectan a los Estados provienen de actores estatales y no estatales que aprovechan el ciberespacio, con la particularidad, en muchos casos, del "anonimato". De ese modo, surge una nueva estrategia de los gobiernos para salvaguardar a sus ciudadanos dentro de las fronteras virtuales del Estado, y llamada *ciberdefensa* (Cano, 2011).

Estas ciberamenazas se potencializan por la masificación del uso de tecnologías de la información que emplean internet y las redes informáticas para generar ciberataques a los Estados; principalmente, a su infraestructura crítica. Por su parte, las Fuerzas Militares (FF. MM.) hacen parte de las capacidades de

seguridad y defensa del Estado; así pues, cumplen su misión constitucional a fin de preservar los intereses nacionales. Es así como la Fuerza Aérea Colombiana (FAC) ha evolucionado hacia una doctrina del poder multidominio, la cual abarca el aire, el espacio y el ciberespacio, como dominios para realizar sus operaciones, por lo que dicha Fuerza es un elemento fundamental dentro de la estrategia de la seguridad multidimensional para enfrentar la amenaza y preservar el interés nacional. En ese sentido, surge la hipótesis de que los intereses del Estado pueden ser afectados por la materialización de las amenazas y desafíos multidimensionales en los dominios aéreo y ciberespacial; al determinar el impacto de dicha afectación, se contribuirá a plantear estrategias para combatir y contener estas amenazas.

Por lo anterior, el presente capítulo busca dar respuesta al interrogante: *¿Cuáles son los impactos que afectan el interés nacional del Estado colombiano en los dominios aéreo y ciberespacial por la materialización de las amenazas y los desafíos multidimensionales?*

Amenazas multidimensionales al Estado nación en los dominios aéreo y ciberespacial

Este acápite centra su atención en las amenazas multidimensionales, y en cómo dichas amenazas afectan al Estado nación en los ambientes aéreo y ciberespacial. Se presenta una descripción conceptual de las amenazas para comprender su relación multidimensional con los intereses nacionales en los dominios aéreo y ciberespacial. Posteriormente, se categorizan las amenazas multidimensionales a partir de su fuente de origen, en relación con los ambientes aéreo, ciberespacial y multidominio. Finalmente, se describen los efectos de estas amenazas en los ambientes aéreo, ciberespacial y multidominio.

Multidimensionalidad

Durante la cuarta plenaria de su Asamblea General, en 2002, la (OEA) declaró: "[…] el concepto y enfoque tradicional debe ampliarse para abarcar amenazas nuevas y no tradicionales, que incluye aspectos políticos, económicos, sociales, de salud y ambientales" (OEA, 2002, p. 1).

De este modo, la *amenaza multidimensional* es entendida como la intención de causar un daño a diferentes sectores del Estado, y su materialización puede

impactar en los intereses nacionales. Con base en las fuentes oficiales de la OEA y la Organización de las Naciones Unidas (ONU), es posible identificar diversas amenazas multidimensionales que afectan el dominio aéreo, y las cuales se detallan seguidamente.

Tráfico ilícito de armas de fuego

Es el traslado, sin la debida autorización, de cualquier arma de fuego de un Estado a otro (OEA, 1997). El tráfico de armas de fuego tiene una conexión directa con otros delitos trasnacionales que ponen en peligro la seguridad de los Estados (Insulza, 2011).

Acceso, posesión y uso de armas de destrucción masiva

Esta amenaza de características catastróficas pone en riesgo, a gran escala, la integridad de las personas, así como la economía de los Estados (OEA, 2020). De esa manera, la OEA señala que parte de dicha amenaza radica en la proliferación, el comercio y el transporte por parte de actores estatales y no estatales.

Degradación del medio ambiente

Se refiere a los cambios y la reducción en la producción de los ecosistemas por acción del ser humano (Abelardo et al., 2013). La materialización de tal amenaza en contra del medio ambiente es de alto impacto en los Estados. Efectivamente, el agua y la biodiversidad son considerados activos estratégicos de la nación, y se requiere, por tanto, a las instituciones del Estado para su defensa y su seguridad (Ministerio de Defensa Nacional [MinDefensa], 2019).

Ahora bien, los anteriores conceptos tienen la misma validez para las amenazas que provienen del ciberespacio; más aún, cuando el uso masivo de la tecnología trae consigo nuevas amenazas, desarrolladas en un nuevo dominio de la guerra, llamado *ciberespacio*, y en el que la ciberseguridad ya no depende exclusivamente del Estado, ni de la ciberdefensa de sus FF. MM. Asimismo, el uso inadecuado del ciberespacio, así como la desprotección y el desconocimiento de este, genera nuevas vulnerabilidades para el Estado nación (Arreola, 2018).

El control y la seguridad de la información se convierten, entonces, en parte de los intereses del Estado, frente a un sistema internacional potencialmente interconectado y que ofrece facilidades para acceder a la información y al control de infraestructura crítica a través del ciberespacio, y no solo por parte de otros

Estados, sino también, por parte de individuos, organizaciones no estatales y grupos con intereses específicos en causar daño al Estado. Sumado a lo anterior, el ciberespacio ha desdibujado las fronteras entre los Estados, lo cual afecta el concepto de soberanía y dificulta identificar a los agresores para poder atribuir responsabilidades (Villalba & Corchado, 2017).

La característica de global que tiene el ciberespacio permite que las ciberamenazas sean totalmente válidas para cualquier Estado, toda vez que ellas representan un riesgo y un desafío para su seguridad (Aguilar, 2020).

Ataques a la seguridad cibernética

Son considerados una nueva amenaza; representan, a su vez, una preocupación para la seguridad del hemisferio, pues, dada la posibilidad de sufrirlos, la cooperación entre los Estados se vuelve una condición fundamental para combatirlas (OEA, 2002). En ese sentido, un ataque a la seguridad cibernética es entendido como cualquier acción desarrollada en el ciberespacio que logre destruir, negar, modificar o utilizar los sistemas de información del adversario (Stein, 1996).

Ciberamenaza

La revolución de las comunicaciones trajo consigo grandes ventajas respecto al uso de estas, de modo que trajeron desarrollo y avance a la sociedad. El uso masificado de las comunicaciones crea un nuevo escenario, denominado el ciberespacio (Jiménez, 2015). Realpe y Cano (2020) destacan cómo las ciberamenazas son producto de *tecnologías disruptivas*; un concepto que afecta potencialmente la seguridad y defensa nacional. Por lo anterior, los Estados deben integrar sus instituciones para hacer frente a dicha problemática desde todos los ámbitos.

En tal sentido, una ciberamenaza tiene la capacidad y la intención de causar un daño a los activos de una organización, y puede originarse de manera tanto interna como externa y empleando el ciberespacio para materializarse (Ganuza, 2020).

Terrorismo-ciberterrorismo

La constante mutación de la amenaza la ha llevado a evolucionar mediante el empleo del ciberespacio como una estrategia más del terrorismo convencional, aprovechando el miedo para desestabilizar al Estado por medio de acciones terroristas (Rodríguez, 2012). Ese recurso es válido en el ciberespacio, puesto

que emplea la masificación y el uso de la tecnología para lograr sus objetivos (Buitrago et al., 2017).

El concepto de terrorismo permite clasificar al ciberterrorismo como una amenaza multidimensional en creciente evolución, y que se manifiesta en el dominio del ciberespacio de forma rentable, económica y anónima para obtener beneficios tanto del sector privado como del sector público (Alda Mejías & de Sousa, 2015).

Delincuencia organizada transnacional

Se la define como una organización criminal estructuralmente diseñada y compuesta por tres o más personas que actúan con el propósito de cometer uno o más delitos con fines económicos (Torres, 2013). Así mismo, la OEA (2021) argumenta que esta amenaza representa para el Estado la obligación de proveer seguridad y defensa a sus conciudadanos y sus instituciones, toda vez que se considera a la delincuencia organizada transnacional (DOT) la génesis de las demás amenazas multidimensionales. La DOT tiene la particularidad de ser ejercida por actores no estatales, y representa un desafío para la legislación de cada país, al haberse desdibujado las líneas divisorias entre la seguridad y la defensa, característica que se analizará más adelante.

Problema mundial de las drogas

Esta amenaza, de característica transnacional, es una de las principales actividades de la delincuencia organizada, al igual que una de las actividades ilícitas más lucrativas entre las que ocasionan más problemas a la seguridad de los Estados (OEA, 2021). Dicha amenaza presenta peculiaridades multidominio; al igual que el terrorismo, ha evolucionado y emplea la masificación como el uso de las tecnologías —particularmente, internet— para comercializar las drogas, de manera similar a como se hace desde un sitio web. La diferencia radica en la forma anónima y clandestina que emplea, lo que dificulta el seguimiento por parte de las autoridades (European Monitoring Centre for Drugs and Drug Addition, 2017).

Actos de interferencia ilícita

Son todos aquellos actos hostiles que comprometan la seguridad y la integridad tanto de la infraestructura aeronáutica y la aviación civil del Estado como del personal que interactúa en ella; asimismo, los ataques a la infraestructura cibernética que soporta el Sistema Nacional del Espacio Aéreo (Aerocivil, 2020).

Tabla 1. *Categorización de las amenazas multidimensionales y la afectación en los dominios aéreo y espacial*

Amenazas multidimensionales y su afectación en los dominios aéreo y ciberespacial			
Amenazas multidimensionales	Fuente	Afectación en los dominios	
		Aéreo	Ciberespacial
Tráfico ilícito de armas de fuego	(OEA, 2002) (ONU, 2004)	X	
Degradación del medioambiente	(MDN, 2019)	X	
Acceso, posesión y uso de armas de destrucción masiva	(OEA, 2002) (ONU, 2004) (OEA, 2021)	X	
Ataques a la seguridad cibernética	(OEA, 2020) (OEA, 2021)		X
Terrorismo	(OEA, 2002) (ONU, 2004) (OEA, 2021)	X	
DOT	(OEA, 2002) (ONU, 2004) (OEA, 2021)	X	
Problema mundial de las drogas	(OEA, 2002), (ONU, 2004), (OEA, 2021)	X	
Acto de interferencia ilícita	(RAC160, 2020)	X	

Fuente: elaboración propia, con base en Herrera (2021).

La tabla 1 categoriza las amenazas multidimensionales a partir del momento en que fueron acogidas por la comunidad internacional, en relación con la afectación sobre los intereses transnacionales en los dominios aéreo y ciberespacial y multidominio.

Amenazas multidominio

Con base en la tabla 1, se evidencia cómo existen amenazas multidimensionales que por su constante mutación afectan de manera simultánea los dominios aéreo y ciberespacial. Ejemplo de estas amenazas son el terrorismo, la DOT y el problema mundial de las drogas, todas las cuales afectan los intereses

nacionales en estos dos ambientes. No obstante, debido al actor, la intención y la capacidad para causar daño, las mencionadas amenazas presentan características multidominio, pues su afectación hace presencia en los dos ambientes.

Amenazas multidimensionales que afectan al dominio aéreo

En el uso y la explotación del espacio aéreo se presentan diferentes formas de actuación de actores estatales o ilegales a fin de causar daño y afectación a los intereses nacionales. Ejemplo de lo anterior se considera el transporte aéreo ilegal de armas de fuego, como también, el transporte de armas de destrucción masiva por grupos al margen de la ley o de otros actores Estatales, que pretenden afectar la seguridad nacional desde el dominio aéreo; en consecuencia, se ha evidenciado que su transporte entre otras modalidades se realiza interviniendo la carga aérea (Acuña, 2021).

Al materializarse esas amenazas, el impacto a la soberanía de los Estados se materializa en la violación del espacio aéreo, mediante el uso ilegal de aeronaves para transportar todo tipo de armas. Estas amenazas, igualmente, potencializan otras de carácter multidimensional, como la delincuencia organizada y el terrorismo, que también atentan contra la seguridad y defensa de una nación; por tal motivo, es prioritaria la acción institucional para contenerlas y combatirlas (Castañeda & Torres, 2018).

Por otra parte, las amenazas contra el medio ambiente y los recursos naturales del Estado representan en la actualidad un riesgo alto en cuanto a la pérdida de activos estratégicos. De este modo, las capacidades del poder aéreo de la nación permiten el empleo de medios aéreos, a fin de proveer seguridad y defensa sobre el interés nacional.

Amenazas multidimensionales que afectan el dominio ciberespacial

Las amenazas que afectan el dominio ciberespacial —como el empleo de internet, las redes sociales y el uso de las redes informáticas, entre otros recursos— son medios de innovación que facilitan las comunicaciones (Zárate, 2021). Es una realidad que, en la denominada Cuarta Revolución Industrial, los gobiernos han accedido a la explotación y el uso del ciberespacio permitiendo la interconexión de sus instituciones y, a su vez, la interacción con los demás Estados, en un sistema internacional que se comunica y se interrelaciona cada vez más con el uso de un activo estratégico, como lo es la información a través del ciberespacio.

Amenazas que afectan el ambiente multidominio

El concepto clásico de los *dominios de la guerra* habla de tres dominios en los que se desarrollan las operaciones militares de tierra, mar y aire. La evolución de la tecnología permite expandir este concepto al espacio. Más aún, el uso masivo de las tecnologías de la información y las comunicaciones (TIC) permitió un quinto dominio, llamado ciberespacio. García (2019) expresa cómo estos dominios se agrupan en tres ambientes físicos (tierra, mar y aire), el *dominio de la información* (ciberespacio), el *dominio cognitivo* (la doctrina y la razón) y el *dominio social* (donde se comparte información y se toman decisiones). Todos ellos deben ser tenidos en cuenta de manera especialísima para abordar temas y conceptos de la seguridad nacional. Por su parte, la Organización del Tratado de Atlántico Norte (OTAN), bajo el concepto de *simplicidad en las operaciones*, ha determinado tres *dominios de la guerra*: el *físico*, el *virtual* y el *de opinión* (García, 2018).

El ambiente multidominio cobra importancia a partir de la afectación de amenazas comunes en los dominios aéreo y ciberespacial como el terrorismo, la DOT, el problema mundial de las drogas y los actos de interferencia ilícita.

La necesidad de interconectividad y la relación entre diversos actores se convierten en medios propicios para que los Estados sean blanco de ataques a la seguridad cibernética, y que buscan acceder al control del activo estratégico de la información. De igual manera, el ciberespacio es empleado para atacar a las instituciones que combaten y contienen las amenazas en todos los ambientes operacionales, y las cuales logran generar daños a la infraestructura y a los ciudadanos empleando el ciberterrorismo. El terrorismo convencional en un entorno físico también obtiene una particularidad multidominio.

La DOT y el problema mundial de las drogas ilícitas también han evolucionado, al adquirir características de amenaza multidominio donde el medio aéreo se usa para transportar y traficar, y el ciberespacio, para comercializar estas acciones ilícitas. Lo anterior obliga al control efectivo y al dominio del aire y el ciberespacio de los Estados para combatirlas, y velar así por la integridad de los intereses nacionales.

En resumen, las amenazas multidimensionales logran afectar los dominios del aire y del ciberespacio, y provienen no solo de actores Estatales, también, de la participación de múltiples actores. Al materializarse, las amenazas afectan los intereses nacionales; entre ellos, la soberanía del territorio, la seguridad, la integridad y el bienestar de sus conciudadanos, la estabilidad económica y la

salud pública. De igual manera, la constante evolución de la amenaza emplea la tecnología para causar un efecto más rápido y efectivo y con menores costos, por lo que el ciberespacio se ha convertido en un medio propicio para su materialización. Corresponde, entonces, al Estado hacer frente a dichas amenazas comprendiendo que muchas de ellas, en principio, son responsabilidad de la seguridad pública, pero cuando se materializan tienen impacto en la seguridad nacional.

Los intereses nacionales del Estado colombiano frente a las amenazas multidimensionales en los dominós aéreo y ciberespacial

Este acápite describe la forma como las amenazas multidimensionales se materializan y afectan al Estado nación desde los dominios aéreo y ciberespacial, y desde ambientes multidominio, al igual que los intereses nacionales en el Estado colombiano.

Es de aclarar cómo la Constitución Nacional de Colombia no hace referencia de forma explícita al término *intereses nacionales*; sin embargo, estos son entendidos bajo el concepto *fines esenciales del Estado colombiano*, así:

> Servir a la comunidad, promover la prosperidad general y garantizar la efectividad de los principios, derechos y deberes consagrados en la Constitución; facilitar la participación de todos en las decisiones que los afectan y en la vida económica, política, administrativa y cultural de la Nación; defender la independencia nacional, mantener la integridad territorial y asegurar la convivencia pacífica y la vigencia de un orden justo. (Constitución Política de Colombia, 1991, art 2.)

En complemento a lo dispuesto en la Constitución Política colombiana, y a fin de establecer una clara relación en los dominios aéreo y ciberespacial, se acogen los argumentos de estudios de formulación de los intereses nacionales realizados por la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG) en los que se clasifican los intereses como *estratégicos* y *vitales*, según se muestra en la tabla 2.

Tabla 2. *Clasificación de los intereses nacionales de Colombia*

Intereses nacionales de Colombia	
Intereses estratégicos	**Intereses vitales**
• Desarrollo territorial sostenible con infraestructura de calidad. • Fortalecer la identidad nacional, la cultura, la educación y la innovación. • Preponderancia de las economías lícitas en el territorio nacional. • Protección integral del territorio, y desarrollo marítimo, fluvial y especial del país. • Control efectivo de las fronteras nacionales. • Protección de los activos estratégicos de la nación (recursos hídricos, biodiversidad, infraestructura crítica, etc.).	• Prevención del sistema democrático, sus principios y sus valores. • Presencia integral de la institucionalidad en el territorio nacional. • Prosperidad sostenible. • Seguridad física.

Fuente: elaboración propia, con base en Giraldo y Cabrera (2020).

En la tabla 3 se ilustra el resultado del análisis categorial obtenido de distintas fuentes, y se lo relaciona con las particularidades y las características del Estado colombiano en los dominios aéreo y ciberespacial.

Inicialmente se clasifican las amenazas multidimensionales en el dominio aéreo, y posteriormente, en el dominio del ciberespacio. Al final, se presentan las amenazas que afectan a ambos dominios, o *amenazas multidominio*. Asimismo, se describe la amenaza identificada y la forma como esta se materializa, y por último se la relaciona con el *efecto* y el *impacto*; el efecto refleja el propósito de la amenaza, y el impacto, la consecuencia final sobre los intereses nacionales (Libera, 2007).

Tabla 3. *Formas, efectos e impactos de las amenazas sobre los intereses nacionales del Estado colombiano*

Amenazas multidimensionales en el dominio aéreo			
Amenaza	**Forma**	**Efecto**	**Impacto en los intereses nacionales del Estado colombiano**
Tráfico ilícito de armas de fuego	Uso de medios aéreos para transporte ilegal de armas de fuego	Explotación ilegal del espacio aéreo nacional	Violación de la soberanía nacional y de la seguridad física

Degradación del medio ambiente	• Minería ilegal • Deforestación • Cultivos ilícitos	• Contaminación ambiental • Desastres naturales • Tráfico de drogas	Pérdida de activos estratégicos y vitales de la nación
Acceso, posesión y uso de armas de destrucción masiva	Uso de medios aéreos para el transporte ilegal armas de destrucción masiva	Explotación ilegal del espacio aéreo nacional	Violación de la soberanía nacional y de la seguridad física

Amenazas multidimensionales en el dominio ciberespacial			
Amenaza	**Forma**	**Efecto**	**Impacto en los intereses nacionales del Estado colombiano**
Ataques a la seguridad cibernética	• *Malware* • Distributed denial of Service • *Phishing* • *Waterinh-hole* • *Ransomware*	• Pérdida o daño a la infraestructura crítica • Colapso económico	• Violación a la soberanía y la independencia nacionales • Pérdida de la integridad territorial. • Pérdida de los derechos y las libertades de los colombianos

Amenazas multidominio			
Amenaza	**Forma**	**Efecto**	**Impacto en los intereses nacionales del Estado colombiano**
Terrorismo	Ataque terrorista Ataque ciberterrorista	• Daño a la infraestructura crítica • Daño a los ecosistemas y a la biodiversidad • Daño en el capital humano • Afectación económica	• Pérdida de los derechos y las libertades de los colombianos • Pérdida de recursos vitales • Pérdida de la seguridad nacional • Pérdida de vidas en la sociedad
Delincuencia organizada transnacional	• Tráfico de drogas • Tráfico de armas • Trata de personas • Tráfico de migrantes	• Incentivo a la corrupción • Afectación económica • Daño a los ecosistemas y a la biodiversidad	• Pérdida de la convivencia pacífica • Pérdida de la seguridad nacional

Problema mundial de las drogas	Tráfico de drogas	• Incentivo en la corrupción • Afectación económica • Daño a los ecosistemas y a la biodiversidad • Preponderancia de las economías ilícitas	• Pérdida de la convivencia pacífica. • Pérdida de la seguridad nacional
Actos de interferencia ilícita	• Apoderamiento, destrucción o intrusión de aeronaves • Toma de rehenes	• Daño a la infraestructura crítica aeronáutica • Afectación a la población	• Pérdida de la seguridad nacional. • Pérdida de la libertad y de vidas en la sociedad

Fuente: elaboración propia.

Amenazas multidimensionales en el dominio aéreo colombiano

Tráfico ilícito de armas de fuego

En Colombia, el tráfico ilícito de armas de fuego tiene dos particularidades: primero, la posición geoestratégica del país, que facilita la conexión con América Central y con Norteamérica; y segundo, el aprovisionamiento de armas de fuego para los grupos al margen de la ley dentro del conflicto interno colombiano. Las rutas aéreas en Colombia son empleadas para el tráfico de armas ilícitas; especialmente, en las fronteras, donde no hay acceso por vía terrestre, ya que la espesa vegetación impide el control por parte de las autoridades, situación que es aprovechada por los traficantes.

Los traficantes de armas emplean pistas ilegales en los territorios selváticos colombianos; estas provienen de Venezuela y, especialmente, de Brasil por donde ingresa cerca del 50 % del total de armas que llegan a Colombia (ONU, 2007). El transporte de armas ilegales se hace en aeronaves que aterrizan en esas pistas ilícitas, aprovechando espacios de no cobertura de los radares en algunos sectores, o sobrevolando a baja altura para evadirlos. Todo ello equivale a incursionar de manera ilegal en el espacio aéreo colombiano, al ingresar a territorio del país por vía aérea sin ninguna autorización, lo que, con toda claridad,

infringe la soberanía nacional e impacta los intereses vitales de Colombia. De esta manera, corresponde a la FAC, en particular, ejercer el control sobre ese espacio aéreo y defender la soberanía nacional en el ámbito aéreo mediante la vigilancia del espacio aéreo.

En el continente americano, Colombia es el segundo país con mayor incautación de armamento y municiones ilegales, con cerca de 25.000 armas —en su mayoría, armas cortas— que se comercializan en el mercado negro, y de lo cual se ha registrado un aumento considerable a lo largo de los últimos años (ONU, 2020)

Degradación del medio ambiente

Para el caso colombiano, esta amenaza multidimensional se presenta de tres maneras. Una de ellas es la minería ilegal, mediante el uso de los recursos mineros —especialmente, el oro—, lo que no solo se hace de manera criminal, sino que emplea para su extracción métodos que contaminan el medio ambiente —sobre todo, los ríos— con materiales tóxicos como el mercurio, que es altamente nocivo para la salud. Entre 2018 y 2019, Colombia perdió alrededor de 6.669 hectáreas de cobertura vegetal a causa del uso de maquinaria pesada para la extracción de minerales (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2020).

Por otra parte, la deforestación y los cultivos ilícitos están directamente relacionados, toda vez que buscan, principalmente, la producción de insumos para fabricar drogas ilícitas. En 2020, Colombia perdió 171.685 hectáreas de bosque natural; la selva amazónica fue el ecosistema más afectado (*El Tiempo*, 2021a).

En consecuencia, los efectos de la materialización de estas amenazas en Colombia han sido la contaminación ambiental —en especial, ríos y peces—, los desastres naturales y el tráfico de drogas como las principales consecuencias medioamentales de los cultivos ilícitos, lo que representa, a su vez, un impacto sobre los intereses estratégicos de Colombia, como la protección de activos estratégicos de la nación. Ejemplo de dicho compromiso del Estado es la participación de la FAC para "Contribuir a la consolidación del control institucional del territorio y la protección de los recursos naturales" (Fuerza Aérea Colombiana [FAC], 2020a, p. 66).

Acceso, posesión y uso de armas de destrucción masiva

La evolución del conflicto interno colombiano trajo consigo innumerables modalidades técnicas y tácticas empleadas por los grupos al margen de la ley en

cuanto al uso de armas en contra de las fuerzas del Estado. Ejemplo de ello son los cilindros bomba, dentro de los cuales se almacenaban sustancias químicas mezcladas con elementos metálicos (metralla), y sustancias biológicas, como materia fecal (Hernández, 2018). Estos artefactos explosivos improvisados (AEI) eran dirigidos contra la población civil y las FF. MM., y causaban una afectación en masa apoyada por el terror. Si bien es cierto que en Colombia no se tienen registros oficiales sobre el acceso, la posesión o el uso de armas de destrucción masiva sofisticadas, no puede dejarse de lado tal amenaza; por el contrario, el Estado colombiano debe prepararse para su eventual aparición y su consecuente afectación a la seguridad, tanto pública como nacional, y de la cual el transporte por vía aérea es uno de los medios para su proliferación o su ingreso al país, lo que, a su vez, viola la soberanía nacional.

Amenazas multidimensionales en el dominio ciberespacial colombiano

Ataques a la seguridad cibernética

Las ciberamenazas evolucionan rápidamente y con una complejidad cada vez mayor, toda vez que provienen de distintos actores —ya sean estatales, ilegales o comunes—, dependiendo tanto de la capacidad para causar un daño como del efecto que este pueda generar. Los ataques cibernéticos son eficientes en términos de costos y esfuerzo para su ejecución, con beneficios representativos en los sectores tanto públicos como privados y estatales, por lo cual sus ejecutores asumen un bajo riesgo (Alda Mejías & de Souza, 2015).

El *ciberataque* es entendido como la acción, por parte de un ser humano, de manera directa o a través de un sistema programado, para afectar o dañar de manera perjudicial los elementos presentes en el ciberespacio del enemigo, buscando así causar un efecto directo sobre la disponibilidad de la información o sobre infraestructuras críticas (Ganuza, 2020).

Al mismo tiempo, la amenaza de ciberataque se encuentra dentro del sexto riesgo a escala mundial, precedida de los riesgos de clima extremo, fracaso de la acción climática, daño al medio ambiente, enfermedades infecciosas y pérdida de la biodiversidad, que impactan directamente la estabilidad económica de los Estados, y provoca, a su vez, una competencia geoestratégica en el sistema internacional que pone en alerta sobre la seguridad y defensa de estos (Foro Económico Mundial, 2020).

La tabla 4 permite identificar diferentes amenazas relacionadas con ataques a la seguridad cibernética, las cuales pueden materializarse de distintas formas, y logran, igualmente, impactar los intereses nacionales del Estado colombiano en el dominio ciberespacial.

Tabla 4. *Clasificación de ciberamenazas, y la forma como se materializan*

Ciberamenaza	
Clase de ciberamenaza	**Formas**
Ciberespionaje	*Malware* Distributed denial of Service *Phishing* *Waterinh-hole* *Ransomware*
Ataque a infraestructura crítica	
Ingeniería social	
Hacktivismo	
Ciberguerra	
Amenaza persistente avanzada	

Fuente: elaboración propia.

Tabla 5. *Descripción de la forma como se materializan algunas ciberamenazas*

Forma	Descripción
Phishing	Ciberataque diseñado para engañar a una persona emulando sitios y fuentes oficiales —generalmente, por vía e-mail—, para que la víctima proporcione información confidencial o privada, como números de tarjetas de crédito, usuarios y contraseñas, e información bancaria, entre otros.
Malware	Software malicioso diseñado para afectar un sistema informático.
Watering hole	Es una forma de ciberataque en la que se pretende engañar a un grupo de personas infectando los sitios web que estas frecuentan, con el objetivo de acceder a información confidencial para emplearla en ciberoperaciones.
Distributed denial of Service	El ataque de denegación de servicio (ataque DoS) es un tipo de ciberataque que busca sobrecargar un sistema, una máquina o un recurso de red mediante solicitudes que se generan en masa, para así lograr que este quede fuera de servicio.

Forma	Descripción
Ransomware	Es un tipo de ciberataque en el que, habitualmente, por medio del cifrado de ficheros, la información es secuestrada, y después la víctima es amenazada con la publicación de su información o la eliminación permanente de estos.

Fuente: elaboración propia, con base en Ganuza (2020).

Ciberespionaje

Este tipo de ciberamenaza va dirigida, generalmente, hacia los Estados, buscando obtener información que permita conocer datos de carácter económico, político, geoestratégico y militar (Villalba & Corchado, 2017). El ciberespionaje es perpetuado por agencias de inteligencia de los Estados, y Colombia no es ajena a dicha amenaza, por cuanto hay una persistencia de carácter externo para atentar contra los intereses del país (Congreso de la República de Colombia, 2021).

Uno de los casos conocidos de ciberespionaje en Colombia tiene que ver con el robo y el sabotaje de información por parte del *hacker* Andrés Sepúlveda, quién infiltró campañas presidenciales y el proceso de paz en La Habana en 2014 (Tigreros, 2019). Los casos de ciberespionaje generalmente emplean el *phishing* y el *ransomware* como formas para acceder a la información (Villalba & Corchado, 2017). En tal sentido, se emplean los correos electrónicos de los funcionarios de las instituciones para lograr infiltrarse y sabotear o sustraer la información.

Ataque a la infraestructura crítica

La infraestructura crítica de una nación la componen todos aquellos sectores tanto públicos como privados que sostienen el desarrollo y el funcionamiento mínimo y vital que requiere un Estado para su supervivencia en el sistema internacional. Frente a ese concepto, se definen ocho sectores que son vitales para una nación, con miras a su sostenimiento: las plantas de producción de energía; la producción y el suministro de gas y de petróleo; el sector de las telecomunicaciones; el sector financiero; los servicios de suministro y abastecimiento de agua; el sector del transporte; los servicios de emergencia, y la gobernabilidad del Estado (Congreso de los Estados Unidos , 1998).

Al respecto, conviene decir que la sofisticación con la cual se ejecutan los ciberataques es cada día más compleja e incierta: fue el caso, por ejemplo, de la creación del *malware* (virus informático) de STUXNET, en 2010, y que atacó la

planta nuclear de Natanz, en Irán, donde saboteó y destruyó los centrifugadores de uranio, por lo que fue considerado la primera ciberarma de la historia. Al no ser ajeno a esta realidad, el Gobierno de Colombia, a fin de prepararse ante la aparición de esta ciberamenaza, hizo un catálogo de la infraestructura crítica del país, bajo la responsabilidad del Ministerio de Defensa Nacional (MDN), para su protección y su defensa (Consejo Nacional de Política Económica y Social [CONPES], 2016).

Ingeniería social

Esta amenaza se fundamenta en la manipulación de usuarios legítimos en el sistema, para acceder a la información privilegiada; asimismo, se basa en las características de respuesta a emociones por parte del ser humano identificándolo como el eslabón más débil dentro de la cadena de la ciberseguridad (Monsalve, 2018). De esta manera, el correo electrónico es uno de los medios más empleados para que dichas amenazas se materialicen por medio del *phishing*, donde los atacantes se hacen pasar por entidades reconocidas para ganarse la confianza de sus víctimas; por lo tanto, los funcionarios de las instituciones del Estado no se salvan de ser blanco potencial de este tipo de amenazas, con las que se puede acceder a ellos a fin de obtener credenciales de acceso a los sistemas informáticos del Estado.

De ahí que en Colombia el tercer delito cibernético más denunciado sea el acceso abusivo a los sistemas informáticos, donde los atacantes emplean la ingeniería social para acceder a ellos (Policía Nacional de Colombia, 2020).

El hacktivísmo

Se lo define como la relación existente entre el activismo político y el *hacking* sacando ventajas con el uso del ciberespacio. Una de ellas es el anonimato, el cual emplea tácticas delictivas para lograr sus objetivos (Torres, 2018). Esta amenaza de tipo anarquista busca influenciar a la sociedad sobre cierto tipo de comportamientos, decisiones y formas de pensar — en algunos casos, empleando noticias falsas— con el fin de incentivar reacciones mediáticas y sociales. El Estado colombiano fue víctima de este tipo ciberamenaza durante el desarrollo de las protestas sociales, cuando el grupo hacktivista Anonymous se atribuyó el hackeo de páginas web del Estado y el acceso abusivo a información confidencial de altos funcionarios del Gobierno, incluidos el presidente de la República y su ministro de Defensa (*El Tiempo*, 2021b).

En efecto, las páginas gubernamentales fueron atacadas mediante la denegación de servicios, o DDoS (*Semana*, 2021a). Es de esa forma como los atacantes, empleando distintos servidores en todo el mundo, acceden simultáneamente a una página web para lograr que, ante el gran flujo de millones de accesos simultáneos, esta colapse y quede fuera de servicio.

La ciberguerra

Clarke y Knake (2010) la definen como la forma de futuras guerras en que las vulnerabilidades de las tecnologías de la información y el acceso a ellas se convierten en amenazas para la seguridad nacional, y generan así un nuevo concepto de conflicto, que es librado desde el ciberespacio sin la intervención física del ser humano. Por lo tanto, el concepto de la ciberguerra es determinado por el ciberespacio, donde se llevan a cabo acciones bélicas con resultados físicos y tangibles altamente probables sobre infraestructuras críticas empleando redes informáticas o internet.

En este sentido, el concepto de ciberguerra cobra valor al existir un enfrentamiento bélico entre dos o más Estados empleando el ciberespacio para desarrollar operaciones militares, razón por la cual la ciberdefensa cobra un papel decisivo en la protección de los intereses nacionales, al ser las infraestructuras críticas un objetivo de alto valor estratégico, y a las cuales el Estado debe brindar toda la protección requerida. Por tal motivo, en Colombia se crearon el Comando Conjunto Cibernético (CCOC) de las FF. MM., el Centro Cibernético Policial (CCP) y el Grupo de Respuesta a Emergencia Cibernéticas de Colombia (colCERT); todos ellos interactúan para hacer frente a esta ciberamenaza de la guerra en el ciberespacio (Comando General de las Fuerzs Militares [CGFM], 2016).

Amenaza persistente avanzada

Estas ciberamenazas se caracterizan porque los atacantes poseen avanzados conocimientos y recursos para interactuar con sus objetivos y aprender de ellos, para descubrir vulnerabilidades que luego serán usadas para efectuar el ataque (Presidencia de Gobierno de España, 2019). Por esta razón, el tiempo no es una barrera, sino, al contrario, un aliado, por lo que dichas amenazas persisten en el tiempo, de manera que sus víctimas no logren identificar que fueron vulneradas. Por otro lado, Cano (2017) expone que esta ciberamenaza busca acceder a la infraestructura tecnológica de una organización valiéndose de la mayor vulnerabilidad que tienen los sistemas de información: el ser humano.

En tal sentido, los argumentos mencionados cobran valor toda vez que las amenazas persistentes avanzadas fueron desarrolladas para lograr objetivos específicos, complejos y de alto valor estratégico de los Estados. Y Colombia también puede ser víctima de este tipo de ciberamenazas; el resultado será lograr el acceso a información de seguridad nacional, de propiedad intelectual, secretos de Estado y planes de guerra (Cortés, 2017).

Amenazas multidominio en el Estado colombiano

Terrorismo

Esta amenaza apareció en Colombia durante las décadas de 1980 y 1990, cuando adquirió una importancia sin precedentes en el país, toda vez que, el poder adquisitivo del negocio del narcotráfico permitió el uso de la violencia y el terror en contra de la sociedad colombiana y las instituciones del Estado que luchaban para combatir este flagelo (Borrero, 2018). Así las cosas, la infraestructura aeronáutica de Colombia no fue ajena a la situación: tan solo por mencionar algunos casos de ataques terroristas, se encuentran el vuelo 203 de Avianca, que explotó en pleno vuelo cuatro minutos después de su decolaje, en 1989 (Ríos, s.f.). Asimismo, el lanzamiento de cilindros bomba a las instalaciones de la Escuela Militar de Aviación Marco Fidel Suárez, en 1999 (*El Tiempo*, 1999), y el más reciente atentado terrorista al Grupo Aéreo del Casanare, en 2020.

Esta amenaza ha evolucionado dinámicamente, pues ha logrado trasladarse al ciberespacio para materializarse; la infraestructura aeronáutica de una nación es un blanco de alto valor, dadas sus características estratégicas intrínsecas a los intereses nacionales, por lo que no deben descartarse ataques ciberterroristas a los sistemas de comunicación, a la navegación, a la información de las torres de control u otros elementos del poder aéreo de Colombia que se encuentran soportados en el ciberespacio, y que en caso de concretarse podrían llevar a desviar vuelos, apagar radares o generar accidentes aéreos, lo que causaría un impacto a los intereses nacionales, por la pérdida de la seguridad del Estado.

Lo anterior permite determinar que la amenaza del terrorismo se ha materializado en el dominio aéreo mediante la afectación de la infraestructura aeronáutica a través de ataques directos con métodos convencionales; asimismo, puede afectar el dominio ciberespacial empleando ciberamenazas que logren penetrar los sistemas informáticos de la aviación para afectarla. En ambos

casos, la materialización de la amenaza del terrorismo en los dos ambientes causaría un impacto a los intereses nacionales, por la pérdida de la seguridad del Estado.

Delincuencia organizada transnacional

Actualmente Colombia se encuentra en una fase de posconflicto, al firmarse un proceso de paz con uno de los grupos insurgentes —el más antiguo del continente—, denominado Fuerzas Armadas Revolucionarias de Colombia (FARC). Esto lleva a que muchos de los desmovilizados de dicho grupo terrorista retornen a la delincuencia organizada, y fortalezcan así antiguos grupos criminales (Fernández, 2020). En consecuencia, su accionar delictivo se relaciona con otras amenazas multidimensionales, como el narcotráfico, el tráfico ilegal de armas, la minería ilegal, la trata de personas y el lavado de activos, entre otros; evidencias, según lo tratado líneas arriba, cómo estas actividades impactan los intereses nacionales.

Ahora bien, la DOT tiene la particularidad de efectuar sus transacciones a través del ciberespacio, donde los criminales encuentran en la tecnología la manera de alcanzar una característica a escala global; asimismo, el uso de una infraestructura sofisticada con exploradores web, como Tor, sumado al uso del bitcoin como medio de pago, hace que este tipo de transacciones sean por completo anónimas y propicias, para que los Estados no puedan hacer seguimiento efectivo a sus acciones delictivas (Popper, 2019).

Problema mundial de las drogas

Colombia es uno de los mayores productores de hoja de coca en el mundo. Dicha particularidad potencializa el problema mundial de las drogas, toda vez que de este flagelo se derivan otras amenazas, como el tráfico de drogas, la violencia, el terrorismo, el lavado de activos, la corrupción y la degradación del medio ambiente, entre otros. Para 2020, Colombia reportó 143.000 hectáreas sembradas con hoja de coca; o sea, el 7 % menos que el año inmediatamente anterior (UNODC, 2021). Los esfuerzos realizados en Colombia por combatir este flagelo son innumerables. Sin embargo, las rutas aéreas siguen siendo las formas más utilizadas por el tráfico de drogas como respuesta a la creciente demanda mundial de nuevos mercados. La FAC, de forma permanente, ejerce el control del espacio aéreo nacional, intercepta aeronaves que violan el espacio aéreo colombiano y destruye pistas ilegales. A pesar de ello, surgen nuevas rutas para el tráfico de drogas, lo que genera un ambiente dinámico y adaptativo para del Estado colombiano (Ministerio de Justicia y del Derecho, s.f.).

En ese orden de ideas, esta amenaza ha evolucionado empleando el ciberespacio para realizar sus acciones delictivas; un espacio en el que los consumidores tienen facilidad de acceso al mercado de drogas en la web, y los traficantes, la tranquilidad de hacer transacciones virtuales respaldadas por criptomonedas, que garantizan el anonimato (García, 2017).

Este fenómeno irradia a la sociedad y a las instituciones del Estado, y así pone en riesgo la convivencia pacífica, la seguridad nacional y la preponderancia de las economías lícitas del país. Esta amenaza, de características dinámicas y cambiantes, impacta los intereses nacionales desde los dominios aéreo y ciberespacial.

Actos de interferencia ilícita

La aviación civil hace parte del poder aéreo de la nación, y este, a su vez, es empleado para defender y proteger los intereses nacionales; en tal sentido, la amenaza de actos de interferencia ilícita en Colombia ha sido evidente, al registrarse varios casos de secuestro de aeronaves, como lo sucedido al vuelo 602 de la aerolínea SAM, en mayo de 1973 (VOLAVI, 2009); el vuelo 9463 de la aerolínea Avianca, en 1999 (*El Tiempo*, 2019); el avión Dornier FAC 1165 de la empresa Satena, el 31 de enero de 2001 (*El Tiempo*, 2001)), y el avión HK3951 de la aerolínea Aires, en 2002 (*Semana*, 2016). Todos estos, con pasajeros a bordo.

Por su parte, y con base en los reglamentos aeronáuticos internacionales y nacionales, se consideran afectaciones al dominio aéreo y ciberespacial los actos o las intenciones de atentar contra la seguridad de la aviación civil. Aunque en Colombia, por ahora, no se tienen registros de interferencia ilícita a través del ciberespacio, el Reglamento Aeronáutico de Colombia contempla dicha amenaza. Por otra parte, en el resto del mundo sí se ha presentado este tipo de ciberamenazas: como lo ocurrido en el aeropuerto de Bristol, Inglaterra, en 2018, cuando las pantallas informativas fueron hackeadas con un *ransomware* que ocasionó el colapso y los retrasos de los vuelos (*Europapress*, 2018).

En resumen, el Estado colombiano, en concordancia con la Carta Magna, determina cuáles son los fines o los intereses nacionales necesarios para su desarrollo, su crecimiento y la competencia en el sistema internacional. La existencia de amenazas multidimensionales se materializa en el dominio aéreo, en el dominio ciberespacial o en ambos simultáneamente. Por consiguiente, en el siguiente acápite se identifican algunas capacidades con las que el Estado colombiano cuenta, y otras que se requieren, para enfrentarlas y combatirlas.

Capacidades del Estado nación para contener y combatir las amenazas multidimensionales con el poder aéreo y el ciberespacial

En acápites anteriores se identificaron las amenazas multidimensionales que afectan los intereses del Estado colombiano en los dominios aéreo, ciberespacial y multidominio; igualmente, las formas como dichas amenazas se materializan, y los efectos y el impacto sobre los intereses nacionales.

A continuación, se plantean las capacidades que el Estado colombiano debe fortalecer y desarrollar para contener y combatir las amenazas multidimensionales en los ambientes aéreo, ciberespacial y multidominio, toda vez que, al materializarse, afectan de manera significativa el interés nacional de orden estratégico o vital.

Sin embargo, es importante abordar el concepto *capacidad* para comprender la relación de esta con la necesidad de contener y combatir una amenaza. A partir de las múltiples definiciones establecidas, se acogen las siguientes: La Real Academia de la Lengua Española (RAE) define una capacidad como la oportunidad, el lugar o el medio para ejecutar algo. Asimismo, una capacidad puede ser entendida como la actitud de una persona o una institución para llevar a cabo una tarea ("Capacidad", 2021). Por su parte, el Diccionario Político, Estratégico y Militar de la Escuela Superior de Guerra define la capacidad como la suficiencia para ejecutar un curso de acción determinado (Santos & Pardo, 2010); igualmente, la vincula con la ejecución bajo un principio sobre el cual descansa la acción estratégica, y que es la adecuación y la coordinación de los medios disponibles para el cumplimiento de una misión (Santos & Pardo, 2010).

En el mismo sentido, para lograr los objetivos estratégicos de la nación, y proveerla de capacidades requeridas para la protección y la defensa de los fines del Estado, el MDN de Colombia desarrolló el Modelo de Planeación y Desarrollo de Capacidades de la Fuerza Pública, el cual involucra varios componentes, como la Doctrina, la Organización, el Material y Equipo, el Personal y la Infraestructura; estos componentes se conocen con la sigla DOMPI (Ministerio de Defensa Nacional [MinDefensa], 2018).

Por lo tanto, el modelo conceptúa la capacidad como una habilidad que posee una unidad militar o policial empleando el DOMPI para ejecutarla. Dichas habilidades son clasificadas según la naturaleza y el propósito, y empleadas por niveles a las que se le denominan taxonomía de capacidades, a fin de facilitar la

acción de las fuerzas para el cumplimiento de sus misiones y responder a la naturaleza y la especialización de cada una de ellas. Las capacidades se clasifican en *operacionales* y *organizacionales* (MinDefensa, 2018).

Definido el concepto de capacidad y entendido el modelo (CAPACITAS) aplicado en el (MDN), acto seguido la información que se muestra en la tabla 6 permite relacionar los dominios aéreo y ciberespacial con los marcos constitucional, legal, institucional, doctrinario y operacional, a fin de ser tenidos como punto de partida en el planteamiento de las capacidades que debe adoptar el Estado colombiano para la defensa de sus intereses nacionales frente a las amenazas multidimensionales en los dominios aéreo y ciberespacial.

Tabla 6. *Relación de los dominios aéreo y ciberespacial de la nación con los marcos referenciales*

Dominios / marcos	Marco constitucional y legal	Marco institucional y doctrinario	Marco operacional
Dominio aéreo	• Constitución Política de la República de Colombia (1991) (art. 217). • Ley 126 de 1919 creó la FAC). • Ley 89 de 1938 (creó la Aeronáutica Civil Colombiana). • Ley 1955 de 2019 (expidió el Plan Nacional de Desarrollo 2018-2022). • Decreto 2171 de 1992 (creó la Unidad Administrativa Especial de Aeronáutica Civil ([UAEAC]). • Decreto 2937 de 2010 (designó a la FAC como autoridad aeronáutica de la aviación de Estado y ente coordinador ante la autoridad Aeronáutica Civil Colombiana, y constituyó el Comité Interinstitucional de la Aviación de Estado). • Decreto 1000 del 5 de noviembre de 1981, mediante el cual se organiza un cuerpo de Policía Nacional. • Decreto 1400 del 8 de julio de 2002 (creó la Comisión Intersectorial de Seguridad Aeroportuaria de la Aviación Civil).	• Guía de Planeamiento Estratégico Sector de Defensa y Seguridad Nacional, 2019-2022. • Plan Estratégico Militar (PEM) (2030). • Plan Estratégico Institucional del COGFM (2019-2022). • Manual Fundamental de Doctrina Conjunta, MFC-1,0 (2018). • Estrategia para el desarrollo aéreo y espacial de la FAC 2042. • Manual de Doctrina Básica, Espacial y Ciberespacial (quinta edición, 2020). • Guía Metodológica-Planeación por Capacidades del MDN, 2018. • Plan Estratégico Institucional PONAL (2019-2022). • Reglamento Aeronáutico Colombiano, (RAC) (2017).	• Política de Defensa y Seguridad Nacional (2019-2022). • Plan Bicentenario Héroes de la Libertad, FF. MM. 2019 • Plan de Campaña Fuerza Aérea Colombiana. • CCOFA. • CCOBA. • CACOM. • ACUARIO. • Seguridad Aeroportuaria. • Plan de Acción Policía Nacional. • Policía Aeroportuaria.

Dominios / marcos	Marco constitucional y legal	Marco institucional y doctrinario	Marco operacional
Dominio ciberespacial	• Constitución Política de la República de Colombia (1991) (art. 1, 2.15.20). • Decreto 1078 de 2015. • Política de gobierno digital. • Documento CONPES N.° 3854 Política Nacional de Seguridad Digital.	• Manual 2.0 de Tallin • El derecho internacional aplicable a las operaciones cibernéticas (2017). • Manual de Ciberdefensa Conjunto para las FF. MM. (primera edición, 2016). • Manual de Doctrina Básica, Espacial y Ciberespacial FAC (quinta edición, 2020)	• Política de Defensa y Seguridad Nacional 2019-2022. • Plan Bicentenario Héroes de la Libertad, FF. MM. (2019). • Plan de Campaña Fuerza Aérea Colombiana (2018). • CCOC. • ColCERT. • Centro cibernético PONAL.

Fuente: elaboración propia.

Colombia, como Estado social de derecho, instauró en su Carta Política de 1991 los fines de la nación, y estableció en el artículo 216 de dicha Carta Magna la institucionalidad de las FF. MM. para defenderlos y protegerlos. El Gobierno nacional, por su parte, establece el Plan Nacional de Desarrollo, con estrategias y metas para el sector defensa, a través de la Política de Defensa y Seguridad Nacional, desarrollada, a su vez, mediante los planes estratégicos y operacionales de las FF. MM. y la Policía Nacional (PONAL).

Por otra parte, el Estado colombiano instituyó la Unidad Administrativa Especial de Aeronáutica Civil (UAEAC), adscrita al Ministerio de Transporte, como la responsable de dirigir, organizar, coordinar y regular técnicamente el transporte aéreo, así como para controlar, supervisar y asistir la operación y la navegación aéreas que se realicen dentro del espacio aéreo sometido a la soberanía nacional.

Con lo anterior en mente, y en consideración a la necesidad de contar con capacidades apropiadas para contener y combatir las amenazas multidimensionales, el Estado colombiano, con base en el principio de constitucionalidad, debe fortalecer, desarrollar e implementar nuevas capacidades en el dominio aéreo, toda vez que la mutación y la evolución de estas amenazas, con sus formas de actuación, logran mayor impacto sobre los intereses nacionales.

Capacidades del poder aéreo para enfrentar las amenazas multidimensionales

El Estado colombiano, consciente del riesgo que generan las amenazas multidimensionales sobre sus intereses, desarrolla estrategias para combatirlas o contenerlas, soportadas en cuantiosos recursos económicos, empleados para instaurar nuevas capacidades y fortalecer las existentes. Es así como desde el sector político se implementa legislación a fin de proveer de marco legal el actuar de las FF. MM. en la protección y la defensa de sus intereses. No obstante, es necesario implementar nuevas estrategias de seguridad cooperativa, que permitan enfrentar amenazas comunes, mediante un esfuerzo conjunto entre Colombia y otros países, para disminuir el riesgo sobre los intereses nacionales (Banegas, 2017).

En este sentido, la FAC desarrolla acuerdos de cooperación con el gobierno de Estados Unidos, como el convenio Air Brig Denial (negación del espacio aéreo), el cual tiene como propósito la interceptación de aeronaves que pretendan hacer uso ilegal del espacio aéreo colombiano para materializar las amenazas multidimensionales, como el tráfico ilícito de armas y el de sustancias ilegales (FAC, 2014).

Por lo anterior, la defensa del espacio aéreo es fundamental en la protección de intereses tanto vitales como estratégicos. De esa forma, el desarrollo y la aplicación de medios tecnológicos, según el concepto de independencia tecnológica, genera capacidades de diseño propias, como un mayor nivel de seguridad autónomo para el Estado; permite así reducir costos en la adquisición de nueva tecnología, y en el soporte logístico (MinDefensa, 2017). En orden de ideas, la FAC, por ejemplo, ha desarrollado tecnología aplicada en la fabricación de radares tácticos para la defensa aérea y de superficie (FAC, 2017).

De igual manera, la renovación de los medios aéreos es una prioridad para el Estado colombiano, a fin de ofrecer mayor control del espacio aéreo, y que provea, a su vez, una capacidad defensiva, disuasiva y ofensiva ante la materialización de dichas amenazas multidimensionales. Las aeronaves de combate se constituyen en el activo militar más importante en la defensa de la Nación (*Semana*, 2021b). En ese sentido, Colombia cuenta con aeronaves de superioridad aérea tipo Kfir, pero cuya flota debe ser renovada, por su obsolescencia, frente al poder aéreo de países de la región con mejores características para la defensa nacional; asimismo, debido a su alto costo de sostenimiento, pues a la fecha esos aviones ya tienen más de 30 años de servicio. Por lo tanto, lograr

una capacidad estratégica, como la superioridad aérea, requiere los medios, la tecnología y el soporte aeronáutico apropiados, por cuanto el poder aéreo es una herramienta fundamental para defender los intereses nacionales, y ello se logra a partir de la voluntad política del Estado (Gaitán, 2017).

Por lo tanto, el desarrollo tecnológico en la FAC debe ser la punta de lanza que permita obtener nuevas capacidades en el ambiente aéreo, así como disponer de los suficientes medios aéreos sofisticados e infraestructura aeronáutica (aviación militar y aviación civil) que provean no solo capacidad para la defensa de la nación, sino también, en la seguridad, para contener y combatir las amenazas multidimensionales que impactan el interés nacional. Para lograr este objetivo, es importante desarrollar la metodología del MDN, basada en el planeamiento por capacidades como parte de la estrategia para alcanzar, mantener, proteger y defender los fines del Estado colombiano.

En este sentido, al aplicar la metodología DOMPI en el desarrollo y el fortalecimiento de capacidades para combatir y contener las amenazas multidimensionales que afectan los intereses nacionales desde el dominio aéreo, dichas capacidades deben ser soportadas mediante una doctrina fundamentada en el marco constitucional, legal y operacional (Doctrina); asimismo, con una estructura organizacional de Estado, que involucre el empleo de la aviación de Estado y la aviación civil bajo el concepto *poder aéreo integral de la nación* (Organización), a la vez que permita involucrar, adquirir y desarrollar los medios apropiados para enfrentar las amenazas en contra del Estado (Material y Equipo), con el apoyo del mejor talento humano militar y civil, capacitado para hacer parte de la estructuras organizacionales, operativas y tácticas, en roles de dirección, conducción y desarrollo de tareas en el ambiente de dominio aéreo (Personal) para administrar la infraestructura aeronáutica del Estado que soporta la ejecución de las operaciones aéreas (Infraestructura).

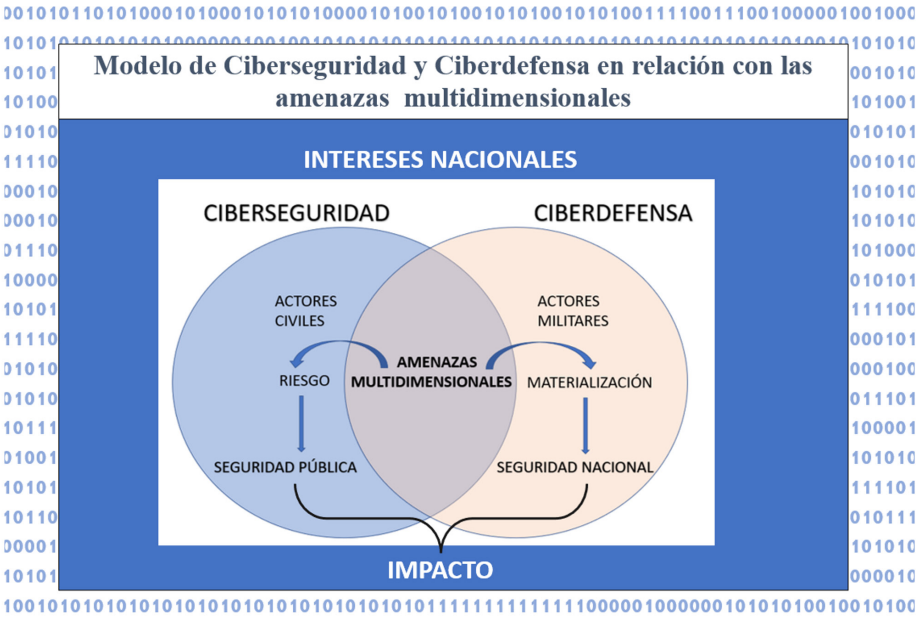
De este modo, una capacidad con la que el Estado colombiano debe contar para combatir y contener las amenazas multidimensionales en el dominio aéreo identificadas en el primer acápite, y descritas en la figura 1, debe ser la modernización de los medios aéreos que hacen parte del sistema de defensa aérea de la nación, que permita un control efectivo del espacio aéreo. De igual manera, fortalecer el desarrollo tecnológico al interior de la Fuerza Aérea Colombiana, como condición fundamental para lograr la autonomía tecnológica que permita la ejecución de operaciones aéreas efectivas en el control del espacio aéreo colombiano.

Capacidades del poder ciberespacial para enfrentar las amenazas multidimensionales

El dominio ciberespacial se ha convertido en parte del interés nacional, por cuanto los Estados han comprendido que, al tener control sobre el ciberespacio, transversalmente se obtiene el dominio aéreo, terrestre, marítimo y espacial. Sin embargo, el surgimiento de este nuevo dominio ha creado también nuevos conceptos sobre la seguridad y defensa de una nación, pues las particularidades del ciberespacio han desdibujado los límites y las responsabilidades de las instituciones del Estado para su defensa.

Argumentado lo anterior, se propone un modelo que involucra el ciberespacio, las amenazas multidimensionales, la seguridad y defensa de los intereses del Estado nación como los factores que intervienen y, en conjunto, conforman un nuevo concepto, el cual permite visualizar y proponer las capacidades con las que Colombia debe contar para enfrentar las amenazas provenientes del ciberespacio y que atenten contra sus intereses.

Figura 1. *Modelo de ciberseguridad y ciberdefensa en relación con las amenazas multidimensionales.*



Fuente: Elaboración propia.

Para Chillier y Freeman (2005), el nuevo concepto de seguridad multidimensional proferido por la OEA no solo es demasiado amplio y difuso, sino que diluye la diferencia entre defensa y seguridad. Si a este concepto se adiciona el factor tecnología, que genera la evolución de nuevas amenazas —especialmente, las que provienen del ciberespacio—, se deduce la existencia de amenazas multidimensionales que producen riesgos a la seguridad pública, y que al materializarse afectan la seguridad nacional. En este contexto, García (2019) afirma que, la tecnología no es exclusiva de militares ni de los civiles, pues en el desarrollo de conflictos en el ciberespacio intervienen estos en conjunto. A su vez, la masificación de esta tecnología hace que dependan de ella infraestructuras tanto militares como civiles de los Estados. Por consiguiente, el concepto tradicional de seguridad y defensa debe ampliar su visión y su comprensión, para así proyectar y obtener capacidades reales y eficaces en la protección y la defensa de los intereses nacionales desde el ciberespacio.

Por otra parte, las amenazas multidimensionales que provienen del ciberespacio son un factor común entre la ciberseguridad y la ciberdefensa, pues al ser identificadas generan un riesgo *para la seguridad pública*, y cuando se materializan afectan *la seguridad nacional*. Para Becerra y León (2019), una de las funciones de la ciberdefensa es proveer la normalidad y la seguridad de una sociedad que interactúa en el ciberespacio en desarrollo de sus actividades cotidianas. Ahora bien, se evidencia cómo el concepto de ciberdefensa abarca características de la seguridad pública; por eso, las ciberamenazas afectan tanto al sector público como al sector privado. En tal sentido, las amenazas que se materializan, ya sea en el ámbito de la seguridad pública o en el ámbito de la seguridad nacional, pueden causar impacto en los intereses estratégicos y vitales del Estado.

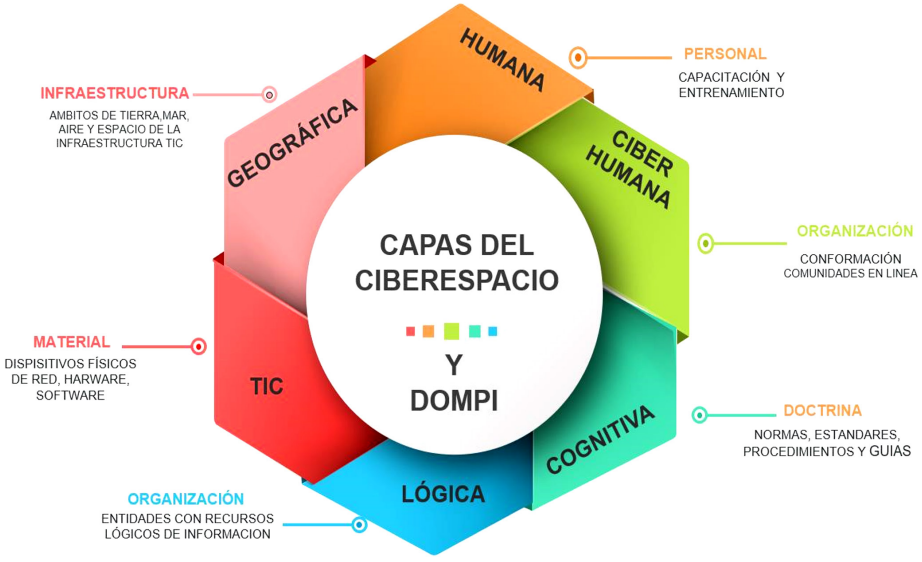
Conviene distinguir cómo en este modelo intervienen distintos actores del ámbito de la ciberseguridad; a saber: civiles que tienen la responsabilidad de proteger infraestructuras al interior del sector privado, y actores estatales a cargo de la protección de los derechos y las libertades de los ciudadanos desde el ciberespacio, como lo hace la PONAL, a través del Centro Cibernético. Por su parte, la institucionalidad del Estado les ha conferido a sus FF. MM. la defensa de la nación, concepto al que, a su vez, no es ajeno el ciberespacio; por lo tanto, en el ámbito de la ciberdefensa corresponde a los militares velar por los intereses de la nación, y han dispuesto para ello el Comando Conjunto Cibernético (CCC).

Una de las características del ciberespacio es la incertidumbre, que dificulta descubrir el origen de las ciberamenazas y la identidad de los atacantes; por

lo tanto, esta incertidumbre puede ser enfrentada mediante el control efectivo del dominio del ciberespacio por parte de los Estados (García, 2019). Así pues, en la ciberseguridad y la ciberdefensa intervienen actores tanto militares como civiles, quienes tienen la responsabilidades y capacidades para ejercer el control ciberespacial.

En ese orden de ideas, se presentan algunas capacidades del poder ciberespacial con las que el Estado colombiano debe contar para combatir y contener amenazas multidimensionales. Dichas amenazas se plantean tomando en cuenta la metodología DOMPI, pretendiendo así analizar las capas que componen el ciberespacio, a fin de identificar en conjunto esas capacidades.

Figura 2. *Planeación de capacidades en relación con las capas que conforman el ciberespacio.*



Fuente: elaboración propia, con base en Ganuza (2020).

En este contexto, Ganuza (2020) expone en la guía de ciberdefensa de la Junta Panamericana de Defensa que el ciberespacio está conformado por distintas capas en las cuales interactúan personas, redes, información, *software*, *hardware* e infraestructura. La primera de dichas capas es la *capa humana*, compuesta por personas. Analizadas estas desde la metodología DOMPI, deben ser entrenadas y capacitadas para interactuar en el ciberespacio (Personal); por

lo tanto, la formación en temas de ciberseguridad y ciberdefensa de los oficiales y los suboficiales, así como del personal civil que integra el MDN, es fundamental para ampliar líneas de investigación (CONPES, 2011). Se evidencia así el fortalecimiento de esta capacidad. La Maestría en Ciberseguridad y Ciberdefensa, de la ESDEG, es el posgrado que actualmente forma oficiales para liderar estrategias que combatan y contengan las amenazas contra el interés nacional provenientes del ciberespacio.

La siguiente capa descrita por Ganuza (2020) es la *ciberhumana*, que se refiere a las personas con una identidad en línea, y las cuales, a su vez, conforman organizaciones virtuales interactuando en el ciberespacio. En Colombia, el (colCERT), el (CCOC) de las FF. MM. y el (CCP) fueron creados por la Política de Ciberseguridad y Ciberdefensa de Colombia. En dichas entidades se desarrollan actividades de control del ciberespacio por parte del Estado, a través de una infraestructura cibernética dispuesta para ello, con la participación de personal que constantemente interactúa en el ciberespacio, a fin de contener ciberamenazas que pretendan afectar e impactar los intereses de la nación, y evidenciando una capacidad fortalecida desde el componente de la organización del modelo DOMPI.

Seguidamente, la *capa cognitiva* abarca los conocimientos adquiridos por las personas, como resultado de su interacción en el ciberespacio; dichos conocimientos son guiados por la doctrina, las normas de actuación, los estándares y los procedimientos por realizar en estas actividades (Ganuza, 2020). En cuanto al marco constitucional legal y la doctrina son elementos fundamentales de una capacidad para emplear el conocimiento en el ciberespacio que permita enfrentar las ciberamenazas. En este sentido, Colombia y sus FF. MM. tienen una doctrina que guía su actuar, como se evidencia en la en la tabla No 6, la relación de los dominios aéreo y ciberespacial de la nación con los marcos referenciales, en sí misma, constituye una capacidad doctrinaria del Estado colombiano.

Por su parte, la *capa lógica* del ciberespacio es, para Ganuza (2020), la información procesada por recursos de computación con los que las organizaciones interactúan entre sí en el ciberespacio. En tal sentido, en el ciberespacio las organizaciones dependen de la información, por lo que las capacidades en dicho componente deber ser orientadas al fortalecimiento de los sistemas de información que garanticen su confidencialidad, su integridad y su disponibilidad, toda vez que la información es un activo estratégico del Estado. Lo anterior, a

su vez, da origen a la Política Nacional de Seguridad Digital, donde la gestión de riesgos de la seguridad digital es la estrategia nacional del Gobierno colombiano para proteger al Estado de ciberamenazas que atenten contra sus intereses (CONPES, 2016).

Seguidamente, se encuentra la *capa de las TIC*, que son todos los dispositivos físicos, electrónicos, *hardware*, *software*, redes cableadas e inalámbricas, computadores, servidores, dispositivos, etc. (Ganuza, 2020).

Esta capa es analizada desde el componente de Material y Equipo, al tratarse del uso de tecnología. Tiene la particularidad de hallarse en constante evolución; indiscutiblemente, una capacidad para adquirir por parte del Estado colombiano es la autosuficiencia tecnológica, a fin de no depender de países externos, toda vez que en el campo de la ciberseguridad y ciberdefensa, dicha autosuficiencia es una variable imposible de subestimar.

Finalmente, se encuentra la *capa geográfica*, como la parte física del ciberespacio donde se encuentra ubicada la infraestructura de las TIC y el lugar físico que habitan las personas que soportan el ciberespacio. Los ambientes geográficos son la tierra, el mar, el aire y el espacio (Ganuza, 2020). Con esto en mente, y acorde con el modelo DOMPI, el componente de la infraestructura determina no solo el fortalecimiento de capacidades de infraestructura física, que contiene, a su vez, la infraestructura TIC, de igual importancia en la defensa y seguridad física de dichas instalaciones, que permiten realizar la ciberseguridad y la ciberdefensa en nombre de la protección de los intereses del Estado desde el ciberespacio. Por lo tanto, una capacidad por fortalecer es la seguridad y defensa de sus instalaciones.

En resumen, el diseño de capacidades con las que el Estado colombiano debe enfrentar las amenazas multidimensionales que afecten el dominio aéreo y el dominio ciberespacial de la nación debe ser concebido mediante la metodología de planeación basada capacidades, la cual permite, mediante los componentes (DOMPI), hacer un análisis prospectivo sobre las capacidades que se deben adquirir o fortalecer. De ahí que la renovación de los medios aéreos y el desarrollo de tecnología propia sean fundamentales para combatir y contener las amenazas en el ámbito del dominio aéreo. Por su parte, las capacidades del dominio ciberespacial están enfocadas en fortalecer las existentes. Sin embargo, desarrollar tecnología autónoma garantiza que las actividades en el ciberespacio desarrolladas por Colombia no dependan de terceros.

Conclusiones

La investigación evidencia, en primer término, el gran volumen documental de carácter teórico-conceptual sobre el tema en cuestión, lo que facilitó el proceso de análisis categorial por núcleos temáticos, para describir, de manera específica, cuáles amenazas multidimensionales son las que afectan el Estado nación en los ambientes aéreo y ciberespacial. A partir de ese hallazgo, fue posible relacionar dichas amenazas con los intereses nacionales. De igual manera, se logró categorizar las amenazas multidimensionales, a partir de su fuente de origen, en relación con los ambientes aéreo, ciberespacial y multidominio. De ese modo, se consiguió establecer los efectos de las mencionadas amenazas en los ambientes aéreo, ciberespacial y multidominio, como también, sus formas y su impacto sobre los intereses nacionales. Finalmente, se proyectaron algunas capacidades que el Estado colombiano debe desarrollar para contener y combatir estas amenazas multidimensionales con los poderes aéreo y ciberespacial.

El marco teórico facilitó el entendimiento de los conceptos relacionados con los núcleos temáticos objeto de análisis, para generar nuevo conocimiento con apoyo en tablas y figuras. Los conceptos desarrollados cobran valor a partir del significado sobre: la amenaza, la multidimensionalidad, la seguridad multidimensional, los intereses nacionales, la ciberseguridad, la ciberdefensa, el poder aéreo, el poder ciber espacial, el Estado nación, el domino aéreo y el domino ciberespacial, entre otros.

El análisis conceptual permitió identificar las características de las amenazas multidimensionales categorizadas bajo el enfoque adoptado por la (OEA) durante la declaración de Bridgetown, en 2002, entendidas como nuevas amenazas de carácter trasnacional, y cómo ellas tienen origen estatal y no estatal, y afectan la seguridad de uno o más Estados, lo que dificulta la forma como se las puede contener o combatir.

La tipificación de las amenazas multidimensionales que afectan los dominios aéreo y ciberespacial tiene su origen en la categorización de organizaciones internacionales como la (ONU y la OEA). Sin embargo, dichas amenazas son consideradas, igualmente, en la doctrina de seguridad y defensa nacional, así como en la normatividad de sectores estatales y no estatales de orden nacional e internacional, asociadas a los dominios aéreo y ciberespacial. Es así como tales amenazas se incluyen en las políticas de gobierno, los manuales de doctrina militar, los planes estratégicos institucionales, los planes operacionales, las normas

y los reglamentos aeronáuticos y ciberespaciales, entre otros. Igualmente, se caracterizan, para su estudio y su análisis, bajo ambientes volátiles, inciertos, complejos y ambiguos (VICA).

Las amenazas multidimensionales consideradas por su afectación al Estado en el dominio Aéreo son: el tráfico ilícito de armas de fuego, la degradación del medio ambiente y el acceso, la posesión y el uso de armas de destrucción masiva. A su vez, una amenaza, identificada como los ataques a la seguridad cibernética, afecta al Estado en el dominio ciberespacial. Sin embargo, y como resultado del análisis, se logró establecer que las siguientes las amenazas multidimensionales son consideradas amenazas multidominio, por sus características de (forma, efecto e impacto), puesto que el terrorismo, la DOT, el problema mundial de las drogas y el acto de interferencia ilícita —esta última, de origen aeronáutico— y la constante mutación afectan simultáneamente los intereses nacionales en los dominios aéreo y ciberespacial.

La constante evolución de las amenazas multidimensionales con el empleo de la tecnología en los ambientes aéreo y ciberespacial genera un efecto rápido, efectivo y a menor costo en su materialización. Por ello, corresponde al Estado hacer frente a tales amenazas, en el entendido de que muchas de ellas, en principio, son de competencia de la seguridad pública, pero cuando se materializan tienen impacto en la seguridad nacional.

Por otra parte, la investigación tuvo como resultado la determinación de los intereses nacionales del Estado colombiano, a partir de los fines consignados en el articulado constitucional, junto a la interpretación teórica argumentada en estudios formales, adelantados en la ESDEG, y en los cuales se establece una clasificación de los intereses nacionales, a partir de su condición estratégica o vital. Lo anterior permitió relacionar los intereses nacionales del Estado colombiano con las amenazas multidimensionales que se materializan en los dominios aéreo, ciberespacial y multidominio. Al identificar las amenazas en los dominios aéreo, ciberespacial o multidominio, junto a la forma como estas se materializan, hace posible determinar el efecto como el impacto final sobre los intereses nacionales estratégicos o vitales del Estado colombiano.

El análisis de las amenazas multidimensionales en el dominio aéreo demuestra cómo estas amenazas emplean diferentes formas, como el uso de medios aéreos para el transporte ilegal de armas de fuego, y el acceso, la posesión y el uso de armas de destrucción masiva, mediante la explotación ilegal del espacio aéreo nacional, lo que constituye la flagrante violación de la soberanía nacional.

Asimismo, con la práctica de minería ilegal, la deforestación de los suelos y la siembra de cultivos ilícitos se afecta el medio ambiente, se causan desastres naturales y se incentiva el tráfico de sustancias ilícitas, con su correspondiente impacto en la pérdida de activos estratégicos y vitales de la nación.

En cuanto a las amenazas multidimensionales en el dominio ciberespacial, se evidencia que estas aplican formas soportadas en la tecnología cibernética, como: el uso de *software* malicioso, o (*malware*); los ataques de denegación de servicio distribuido (DDoS); los engaños para hacer compartir información confidencial (*phishing*); los ataques de abrevadero (*waterinh-hole*), y el secuestro de datos (*ransomware*), con efectos en la pérdida o el daño a la infraestructura crítica y el colapso económico, que, a su vez, causa un alto impacto en la violación a la soberanía y la independencia nacionales, así como la pérdida de la integridad territorial y de los derechos y las libertades de los colombianos.

Un hallazgo importante es la identificación de amenazas multidominio, las que igualmente afectan los intereses nacionales en el nivel estratégico o vital, y por sus características y sus formas, está en capacidad para afectar de manera simultánea los dominios aéreo y ciberespacial. Dichas formas son: el ataque terrorista o ciberterrorista; el tráfico de drogas, armas, personas y migrantes; el apoderamiento, la destrucción o la intrusión de aeronaves, y la toma de rehenes. Todo ello tiene efectos específicos o simultáneos, reflejados en: el daño a la infraestructura crítica, a los ecosistemas y a la biodiversidad; en el daño al capital humano y a la economía, y en el incentivo a la corrupción y a las economías ilícitas. Ocasiona, además: la pérdida de los derechos y las libertades de los ciudadanos, la pérdida de la seguridad nacional, la pérdida de vidas y la pérdida de la convivencia pacífica.

El resultado de los hallazgos de la investigación hizo posible plantear algunas capacidades que el Estado colombiano debe fortalecer, desarrollar e implementar para contener y combatir las amenazas multidimensionales que afectan los intereses nacionales estratégicos y vitales con el empleo de los poderes aéreo y ciberespacial.

El planteamiento de capacidades se elaboró siguiendo la metodología aplicada por el MDN (CAPACITAS), a través de la combinación de los componentes (DOMPI): la doctrina y los documentos que soportan la capacidad, la organización, el material y equipo, el personal y la infraestructura. Estas capacidades se clasifican en diferentes niveles de agregación, de acuerdo con su naturaleza y el propósito de su aplicación (operacional u organizacional).

Al relacionar los dominios aéreo y ciberespacial con los marcos constitucional, legal, institucional, doctrinario y operacional, fue posible identificar, mediante la metodología (DOMPI), las capacidades existentes, y caracterizar las capacidades que, se considera, debe adoptar el Estado colombiano para la defensa de sus intereses nacionales frente a las amenazas multidimensionales en los dominios aéreo y ciberespacial.

De esta forma, es posible deducir que para la defensa de los intereses tanto vitales como estratégicos del Estado colombiano en el domino aéreo, se requiere el control total del espacio aéreo nacional, a partir de la modernización, la adquisición y el empleo eficaces de los medios aéreos que hacen parte del Sistema de Defensa Aérea Nacional, que permitan un control efectivo del espacio aéreo colombiano. Asimismo, fortalecer el desarrollo tecnológico de la FAC, como una condición fundamental de la autonomía tecnológica aeronáutica que facilite la eficiente ejecución de operaciones aéreas en todo el territorio nacional.

Las amenazas multidimensionales que afectan el Estado colombiano en el dominio aéreo deben ser contenidas y combatidas con el poder aéreo del Estado Colombiano, concebido de forma integral, puesto que no es un rol exclusivo de la FAC o de los medios militares aéreos en general. El poder aéreo integral adopta una condición de carácter estratégico para la nación, y se constituye a partir de la sinergia entre diversos actores gubernamentales, militares y privados (Barrero et al., 2017).

El dominio ciberespacial se ha convertido en parte del interés nacional, toda vez que los Estados han comprendido la necesidad de tener control total sobre el ciberespacio para, transversalmente, obtener el dominio aéreo, terrestre, marítimo y espacial.

Las amenazas multidimensionales que provienen del ciberespacio son un factor común entre la ciberseguridad y la ciberdefensa, toda vez que, al ser identificadas, generan un riesgo para la seguridad pública, y cuando se materializan afectan la seguridad nacional. Estas amenazas multidimensionales, la seguridad y defensa de los intereses del Estado nación como los factores que intervienen, en conjunto conforman un nuevo concepto que permite visualizar y proponer capacidades con las que el Estado colombiano debe contar para contenerlas y enfrentarlas en el ciberespacio.

Las capacidades del Estado colombiano para contener y combatir las amenazas multidimensionales que afectan el dominio aéreo y el dominio ciberespacial de la nación se diseñan mediante la aplicación de metodologías como

la planeación basada en capacidades, mediante el análisis de componentes de (DOMPI), para, de esta forma, desarrollar o adquirir sistemas robustos multi-dominio de seguridad y defensa de los intereses nacionales, y así garantizar la supervivencia del Estado nación.

Referencias

Abelardo, R., Torres, S., & Castrillon, W. (2013, abril). *Cortolima*. www.cortolima.gov.co

Acuña, R. (2021, abril). El tráfico ilegal de armas como una amenaza a la seguridad integral del Estado. *Revista Academia de Guerra del Ejercito Ecuatoriano, 14*(1), 56-66.

Aerocivil. (2020). *Reglamentos Aeronáuticos de Colombia*. https://tinyurl.com/bdz6pmsu

Aguilar, J. (2020). La brecha de ciberseguridad en America Latiana frente al contexto global de ciberamenazas. *Revista de Estudios en Seguridad Internacional, 6*(2), 17-43. Recuperado el mayo de 2021, de https://doi.org/10.18847/1.12.2

Alda Mejías, S., & de Sousa Ferreira, S. (2015). *La multidimensionalidad de la seguridad nacional: retos y desafíos de la región para su implementación*. Imprenta Nacional de la AEBOE.

Arreola, A. (2018). *Ciberseguridad nacional en México y sus desafíos*. https://www.researchgate.net/

Banegas, A. (2017). ¿Existen estrategias para combatir las amenazas multidimensionales en la región? *Revista Política y Estrategia*, 89-120.

Barrero, D., Baquero, F., & Gaitán, A. (2017). La seguridad multidimensional y el poder aéreo: doctrinas de la OEA y Fuerza Aérea para fortalecer el desarrollo de la seguridad y la defensa. ¿Cuál es el nuevo panorama de Colombia? *Ciencia y Poder Aéreo*, (149), 72-81.

Becerra, J., & León, I. (2019). La seguridad digital en el entorno de la fuerza pública diagnósticos y amenazasdesde la gestión del riesgo. En G. Medina, *La seguridad en el ciberespacio un desafío para Colombia* (p. 420). Escuela Superior de Guerra.

Borrero, A. (2018). Terrorismo, narcotráfico y delincuencia. *Revista Criminalidad*, 134-138.

Buitrago, P., Sánchez, I., & Mojica, J. (2017). *Escenarios y desafios de la seguridad multidimensional en Colombia*. ESDEGUE.

Cano, J. (2011). Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global. *Sistemas*, 4-7.

Cano, J. (2017). Amenazas persistentes avanzadas,inteligencia y contrainteligencia en un contexto digital. *Sistemas*, 82-88.

Capacidad. (2021, 7 de junio). En *Wikipedia*. https://es.wikipedia.org/wiki/Capacidad

Castañeda, J., & Torres, D. (2018). *Análisis crítico del delito de tráfico de armas en Chile factores, regulación y ajuste a los tratados internacionales para su erradicación* [Tesis]. Universidad de Chile. https://repositorio.uchile.cl/handle/2250/167953

Chillier, G., & Freeman, L. (2005). *El nuevo concepto de seguridad hemisférica de la OEA: Una amenaza en potencia*. WOLA.

Clarke, R., & Knake, R. (2010). *Cyber war, the next threat to nacional security and what do about it*. Haper Collins Publisher.

Comando General de las Fuerzs Militares (CGFM). (2016). *Manual de ciberdefensa conjunta para las Fuerzas Militares de Colombia*. Imprenta y publicaciones de las Fuerzas Militares.

Congreso de la Republica de Colombia. (2021, 12 de agosto). *Boletín de Prensa Comisión de Inteligencia y Contrainteligencia del Congreso*.

Congreso de los Estados Unidos de América. (1998, 5 de agosto). *Directiva Presidencial NSC-63*.

Consejo Nacional de Política Económica y Social (CONPES). (2011, 14 de julio). *CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa*. https://tinyurl.com/385vsdya

Consejo Nacional de Política Económica y Social (CONPES). (2016, 11 de abril). *CONPES 3854. Política nacional de seguridad digital*. https://tinyurl.com/3f3w4kvw

Constitución Política de Colombia [Const.]. Junio 13 de 1991. (Colombia).

Cortés, A. (2017). *Amenazas persistentes avanzadas (APT): modelo de funcionamiento y análisis al caso de estudio Projectsauron*. Universidad Piloto de Colombia.

El Tiempo. (1999, 19 de septiembre). Atentado contra Base Aérea de Cali. https://www.eltiempo.com/archivo/documento/MAM-897563

El Tiempo. (2001, 4 de febrero). Secuestró avión de la FAC para poder escapar. https://tinyurl.com/mr343xtu

El Tiempo. (2019, 12 de abril). Se cumplen 20 años del secuestro del vuelo 9364 de Avianca. https://tinyurl.com/3syntncx

El Tiempo. (2021a, 7 de julio). La deforestación en Colombia creció un 8 % en el 2020, según Gobierno. https://tinyurl.com/mpaexum7

El Tiempo. (2021b, 3 de junio). Anonymous revela datos personales de políticos del Centro Democrático. https://tinyurl.com/29hmxd97

Europapress. (17 de septiembre de 2018). Un ciberataque apaga las pantallas del aeropuerto de Bristol. https://tinyurl.com/4sckhmaj

European Monitoring Centre for Drugs and Drug Addition. (2017). *Drugs and the darknet*. EMCDDA–Europol Joint publications.

Fernández, C. (2020). *Análisis legislativo de la delincuencia organizada en el ordenamiento jurídico colombiano* [Tesis]. Universidad Cooperativa de Colombia. https://tinyurl.com/yvevyr8s

Foro Económico Mundial. (2020). *Informe Global de Riesgos 2020*. https://tinyurl.com/2p82yks4

Fuerza Aérea Colombiana (FAC). (2014, 29 de mayo). Estados Unidos otorga certificación del programa ABD a la Fuerza Aérea Colombiana. https://tinyurl.com/mrjbzway

Fuerza Aérea Colombiana (FAC). (2020a). *Estrategia para el desarrollo aéreo y espacial de la Fuerza Aérea Colombiana 2042*. FAC.

Fuerza Aérea Colombiana. (2017, 9 de mayo). Fuerza Aérea colombiana fabrica primer radar táctico de defensa aérea. https://tinyurl.com/5n7rsy2f

Gaitán, A. (2017). *Pensadores, pioneros y precursores del poder aéreo*. ESDEGUE.

Ganuza, N. (2020). *Ciberdefensa. Orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*. Junta Interamericana de Defensa.

García, D. (2019, 27 de septiembre). *Hacia un nuevo concepto de seguridad en un espacio multidominio: complejidad, guerra y seguridad transdominio*. Instituto Español de Asuntos Estratégicos.

García, F. (2018, febrero). Los nuevos dominios en los que se mueven y moverán los camposde batalla del futuro. *Revista General de Marina*, 11-1120.

García, L. (2017). Narcotráfico en la Darkweb: los criptomercados. *Revista Latinoamericana de Estudios de Seguridad, 21*, 191-206.

Giraldo, H., & Cabrera , F. (2020). Los intereses nacionales de Colombia y su protección: el desafio para una estrategia de seguridad nacional. En E. Pastrana, S. Reith, & F. Cabrera, *Identidad e intereses nacionales de Colombia* (pp. 79-113). ESDEGUE.

Hernández, J. (2018, enero-marzo). Amenazas nucleares, biológicas y químicas, una estrategia de manejo. *Revista Científica General José María Córdova, 16*(21), 17-31.

Herrera, C. (2021). *Contexo global contemporáneo de cara a las amenazas, nuevos retos y desafios multidimensionales*.

Insulza, J. (2011). *La seguridad multidimensional y los retos actuales*. https://tinyurl.com/4tazfay8

Jiménez, L. (2015). *La multidimensionalidad de la seguridad nacional: retos y desafíos de la regiónpara su implementación*. Imprenta Nacional de la AEBOE.

Libera, E. (2007). Impacto, impacto social y evaluación del impacto. *ACIMED, 15*(3).

Ministerio de Defensa Nacional (MinDefensa). (2018, diciembre). *Guía metodológica de planeamiento por capacidades*. https://tinyurl.com/4n68cf2b

Ministerio de Defensa Nacional (MinDefensa). (2019). Política de Seguridad y Defensa. https://tinyurl.com/572h937t

Ministerio de Defensa Nacional. (2017, 17 de marzo). *Radar TADER para la Defensa del Sistema Aéreo de la Nación* [Video]. YouTube. https://www.youtube.com/watch?-v=N2Yx7Wpv-bU

Ministerio de Justicia y del Derecho. (s.f.). *Tráfico*. Obtenido de https://tinyurl.com/2mhp-bkku

Monsalve, J. (2018). Ciberseguridad: principales amenazas en Colombia (ingeniería social, phishing y DoS). Universidad Piloto de Colombia: https://tinyurl.com/mwzh8xhj

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2020). *Colombia explotación de oro de aluvión. Evidencias a partir de percepción remota 2019*. Oficina de las Naciones Unidad contra la Droga y el Delito.

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2021). *Colombia Monitoreo de territorios afectados por cultivos ilícitos 2020*. LEGIS.

Organización de Estados Americanos (OEA). (1997, 13 de noviembre). Convención interamericana contra la fabricación y el tráfico ilícitos de armas de fuego, municiones, explosivos y otros materiales relacionados (A-63). https://tinyurl.com/3ujww66z

Organización de Estados Americanos (OEA). (2002, 4 de junio). *Declaración de Bridgetown: enfoque multidimensional de la seguridad hemisférica*. https://tinyurl.com/5n6nnpxr

Organización de Estados Americanos (OEA). (2020). *OEA*. https://www.oas.org/

Organización de Estados Americanos (OEA). (2021, 21 de julio). *Declaración y resoluciones aprobadas por la asamblea general*. http://www.oas.org/es/sla/docs/AG08273S08.pdf

Organización de Estados Americanos (OEA). (s.f.). *OEA mas derechos para la gente*. http://www.oas.org/es/acerca/ssm.asp

Organización de Naciones Unidas (ONU). (2004). *Un mundo más seguro: la responsabilidad que compartimos Informe del Grupo de alto nivel sobre las amenazas, los desafíos*. New York.

Organización de Naciones Unidas (ONU). (2007). *Violencia, crimen y trafico ilegal de armas en Colombia*. ONU.

Organización de Naciones Unidas (ONU). (2020). *Estudio mundial sobre el trafico de armas de fuego 2020*. ONU.

Policía Nacional de Colombia. (2020). *Tendencias cibercrimen Colombia 2019-2020*. https://tinyurl.com/kxk536nc

Popper, N. (2019, 13 de junio). El narcotráfico en internet: el nuevo reto de la policía. *The New York Times*. https://tinyurl.com/3f6wjyut

Presidencia de Gobierno de España. (2019). *Estrategia Nacional de Ciberseguridad*. Gobierno de España.

Realpe, M., & Cano, J. (2020). *Amenazas Cibernéticas a la Seguridad y Defensa Nacional. Reflexiones y perspectivas en Colombia*. https://tinyurl.com/wwych5u2

Revista Semana. (2016, 19 de febrero). La acción que acabó con el Caguán. https://tinyurl.com/2k8bhd4m

Revista Semana. (2021, 19 de marzo). Los aviones de combate de última tecnología que comprará Colombia. https://tinyurl.com/2bncbzxe

Revista Semana. (2021a, 4 de mayo). Anonymous tumbó las páginas web del Senado y la Presidencia de Colombia. https://tinyurl.com/ytn7hnb4

Ríos, J. (s.f.). Un vuelo de cuatro minutos y una verdad que lleva 31 años en el aire. *El Tiempo*. https://tinyurl.com/b6m5mek9

Rodríguez, T. (2012). El terrorismo y nuevas formas de terrorismo. *Espacios Públicos, 15*(33), 72-95.

Santos, M., & Pardo, C. (2010). *Diccionario Político, Estratégico y Militar*. ESDEGUE.

Stein, G. (1996). *Information Attack*. Air War College.

Tigreros, S. (2019). *Estudio sobre casos de cibercrimen en entidades gubernamentales de Colombia en los últimos 5 años* [Tesis]. UNAD. https://tinyurl.com/bdds8mwa.

Torres, H. (2013). Delincuencia organizada transnacional en Colombia. *Dikaion, 22*(1), 109-130.

Torres, M. (2018). El hacktivismo como estrategia de comunicación: de Anonymous al cibercalifato. *Cuadernos de estrategia 197*, 197-224.

Vera, D., Prieto, P., & Garzón, D. (2020). *La ciberseguridad, la ciberdefensa, la identidad y los intereses nacionales y las Fuerzas Militares de Colombia*. Fundación Konrad Adenauer.

Villalba, A., & Corchado, J. (2017). Analisis de las ciberamenazas. *Cuadernos de Estrategia, 185*, 97-138.

VOLAVI. (2009, 17 de agosto). El secuestro aéreo más largo de Colombia. https://tinyurl.com/yaz47sub

Yoyanes, L. (2016). Ciberseguridad. la colaboración publico privada en la era de la cuarta revolución industrial versus ciberseguridad. *Cuadernos de estratégia*, (185), 11-64.

Zárate, G. (2021). Las nuevas amenazas a la seguridad en el contexto latinoamericano. *Revista Academia de Guerra del Ejército Ecuatoriano*, 35-56.