PODER AÉREO, ESPACIAL Y CIBERESPACIAL

frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano

Fabio Baquero Valdés
(Editor)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Colombia

Universidad Militar Nueva Granada

COLECCIÓN ESTRATEGIA, GEOPOLÍTICA Y CULTURA

Poder aéreo, espacial y ciberespacial

frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano

Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Colombia

SCIENTIÆ · PATRIÆ · FAMILIÆ
UNIVERSIDAD MILITAR
NUEVA GRANADA

Colección Estrategia, Geopolítica y Cultura
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Poder aéreo, espacial y ciberespacial

frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano

Fabio Baquero Valdés
(editor)

Escuela Superior de Guerra "General Rafael Reyes Prieto"
Escuela Militar de Cadetes "General José María Córdova"
Bogotá D.C., 2022

Catalogación en la publicación – Escuela Superior de Guerra "General Rafael Reyes Prieto" / Universidad Militar "Nueva Granada"

Poder aéreo, espacial y ciberespacial : frente a desafíos y amenazas multidimensionales que afectan al estado colombiano / Editor Fabio Baquero Valdés -- Bogotá : Editorial ESDEG, Universidad Militar Nueva Granada, 2022.
249 páginas : ilustraciones, tablas y gráficos; 24 cm.
Incluye bibliografía al final de cada capítulo.

ISBN impreso: 978-628-7602-09-0
E- ISBN: 978-628-7602-10-6

(Colección Estrategia, Geopolítica y Cultura)

1.Poder Aéreo -- Colombia 2.Guerra aérea -- Tácticas -- Colombia 3.Seguridad informática -- Derecho y legislación – Colombia i.Salamanca Rodríguez, Edgar Alexander, Brigadier General (colaborador) ii.Robles Cadavid, Juan Manuel, Coronel (colaborador) iii.Baquero-Valdés, Fabio, Coronel (R)(autor – editor) iv.Ocampo Nahar, Gustavo Adolfo, Mayor General (R) (autor) v.Pinilla Pinillia, Tito Saúl, General (R) (autor) vi.Tovar Zambrano, Martha Beatriz, (autora) vii.Mora Peña, Juan David, (autor) viii.Herrera Ibagos, Carlos Andrés, Teniente Coronel (autor) ix.Barrero Barrero, David, Coronel (R) (autor) x.Mora Gámez, Iván Harvey, Teniente Coronel (autor) xi.Martínez Díaz, José Luis, Teniente Coronel (autor) xii.Conde Mesa, Javier Hernando, Teniente Coronel (R) (autor) xiii.Sierra-Zamora, Paola Alexandra (autora) xiv.Fonseca-Ortiz, Tania Lucia (autora) xv.Martínez Gil, Ana Mayerli (autora) xvi. Colombia. Escuela Superior de Guerra "General Rafael Reyes Prieto (ESDEG) xvii.Colombia. Universidad Militar Nueva Granada

UG630.C7P63 2022
358.423

Registro Catálogo SIBFuP 991255714007231

Archivo descargable en formato MARC en: https://tinyurl.com/esdeg991255714007231

Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano

Primera edición, 2022

Editor:
Fabio Baquero Valdés

Cubierta:
Aldemar Zambrano Torres

Colección Estrategia, Geopolítica y Cultura

ISBN impreso: 978-628-7602-09-0
ISBN digital: 978-628-7602-10-6
DOI: https://doi.org/10.25062/9786287602106

2022 Escuela Superior de Guerra
"General Rafael Reyes Prieto"
Vicedirección de Investigación
Sello Editorial ESDEG
Carrera 11 Nº. 102-50 Bogotá D.C., Colombia
www.esdeglibros.edu.co

2022 Escuela Militar de Cadetes
"General José María Córdova"
Departamento de I+D+i
Sello Editorial ESMIC
Calle 80 Nº. 38-00 Bogotá D.C., Colombia
www.librosesmic.com

Libro electrónico publicado a través de la plataforma Open Monograph Press.
Tiraje de 200 ejemplares
Impreso en Colombia

Libro resultado de investigación de la Escuela Superior de Guerra "General Rafael Reyes Prieto", publicado en coedición con la Escuela Militar de Cadetes "General José María Córdova".

Contenido

Prefacio

Brigadier General **Edgar Alexander Salamanca Rodríguez**
Director de la Escuela Superior de Guerra "General Rafael Reyes Prieto"

La Escuela Superior de Guerra "General Rafael Reyes Prieto" se complace en presentar este nuevo libro resultado de la investigación "*Proyección del Poder Aéreo, Espacial y Ciberespacial frente a las amenazas y desafíos multidimensionales que afectan al Estado colombiano*". Este producto, fue elaborado por investigadores de la Fuerza Aérea Colombiana adscritos al grupo de investigación Masa Crítica, en la línea Estrategia, Geopolítica y Seguridad Hemisférica. El proyecto contó para su desarrollo con el concurso de investigadores del grupo de investigación Centro de Gravedad, de la Escuela Superior de Guerra, a través del proyecto "Desafíos y nuevos escenarios de la seguridad multidimensional en el contexto nacional, regional y hemisférico en el decenio 2015-2025". De igual forma, este proyecto vinculó a investigadores de la Escuela de Altos Estudios Estratégicos Nueva Granada, de la Universidad Militar Nueva Granada.

Este libro contribuye en la construcción de nuevo conocimiento como respuesta a las preocupaciones que enfrenta el Estado Colombiano para enfrentar las amenazas multidimensionales que generan riesgos en sus intereses. Motivo por el cual, la nación colombiana está en la obligación de emplear lo mejor de las capacidades del poder aéreo, el poder ciberespacial y el poder espacial en ambientes multidominio, con el fin de contener y combatir dichas amenazas. Sin embargo, el incremento y la mutación de estas circunstancias de riesgo, mantiene al Estado colombiano en permanente alerta, para negar y/o disuadir estas amenazas multidimensionales.

La Escuela Superior de Guerra considera importante emplear este libro en todos los escenarios como un elemento de análisis, consciente de que lo consignado no se convierte en una limitante a la crítica o el debate, donde la argumentación y respeto por las ideas sean los pilares de la discusión.

Prólogo

Coronel **Juan Manuel Robles Cadavid**
Jefe del Departamento Fuerza Aérea Colombiana
Escuela Superior de Guerra "General Rafael Reyes Prieto"

La investigación estimula el pensamiento crítico y la creatividad. A través de ella, el aprendizaje se revitaliza para dar respuesta a planteamientos complejos, mediante procesos de investigación que requieren organización, aplicación de métodos y técnicas para el logro de resultados exitosos de alta calidad. A partir de esta premisa, el Departamento de la Fuerza Aérea Colombiana de la Escuela Superior de Guerra "General Rafael Reyes Prieto", a través de su equipo de investigadores profesionales y estudiantes, adelantó el proyecto "*Proyección del Poder Aéreo, Espacial y Ciberespacial frente a las amenazas y desafíos multidimensionales que afectan al Estado colombiano*".

Con el propósito de aportar mayor cohesión y cooperación en el desarrollo del proyecto se vincularon investigadores de otros grupos de la Escuela e instituciones de educación superior, toda vez que el concurso de diferentes investigadores ofrece un mayor alcance en la producción de nuevo conocimiento. Así mismo, los nuevos desafíos a la seguridad multidimensional en el contexto nacional, regional y hemisférico vinculan diferentes actores y entidades del Estado e imponen sinergias de análisis de estas amenazas, para generar soluciones integrales de características multidominio.

El objetivo primordial del proyecto es demostrar la importancia del empleo de los poderes aéreo, espacial y ciberespacial, sobre la base de capacidades multidominio en función de la supervivencia del Estado, el desarrollo y la prosperidad de la Nación. Estas capacidades —empleadas también para combatir los riesgos y amenazas multidimensionales que afectan a la nación colombiana—no son de uso exclusivo en fines militares. Por el contrario, contemplarlos en condiciones estratégicas, mediante el empleo eficiente de sus capacidades, fortalece el esfuerzo conjunto y de acción unificada, lo cual permite obtener grandes resultados en función de la seguridad y la defensa nacionales, en la protección de los intereses del Estado Colombiano.

Introducción

Fabio Baquero Valdés
Escuela Superior de Guerra "General Rafael Reyes Prieto"

La investigación "*Proyección del Poder Aéreo, Espacial y Ciberespacial frente a las amenazas y desafíos multidimensionales que afectan el Estado colombiano*" fue desarrollada en la Escuela Superior de Guerra "General Rafael Reyes Prieto" (ESDEG), como respuesta a las problemáticas que plantean las nuevas amenazas externas e internas de interferencia nacional, generadas por actores estatales y no estatales, y los cuales impiden o limitan las aspiraciones, los intereses y los objetivos nacionales.

En consideración a lo anterior, y ante la presencia cada vez mayor de fenómenos de crimen organizado trasnacional (COT) y otras formas de amenaza, surge una situación que preocupa a la sociedad nacional e internacional, al punto de convertirse en un nuevo desafío de alta prioridad. Tal y como lo plantea la Organización de Estados Americanos (OEA),

> […] la delincuencia organizada transnacional, el problema mundial de las drogas, la corrupción, el lavado de activos, el tráfico ilícito de armas, el terrorismo, la trata de personas, las minas antipersona, y conexiones entre ellos" hacen parte de las amenazas, preocupaciones, y otros retos de naturaleza diversa que afectan la seguridad de los Estados del hemisferio. (OEA, 2011, p. 39)

Por tal motivo, la investigación plantea el siguiente interrogante por resolver:

¿Cuál debe ser la Proyección del Poder Aéreo, Espacial y Ciberespacial frente a las amenazas y desafíos multidimensionales que afectan el Estado colombiano, como una estrategia nacional para combatir y contener las amenazas multidimensionales que afectan la supervivencia y el interés nacionales?

La presente investigación consideró como punto de partida la declaración sobre la seguridad en las Américas, adoptada por la OEA en octubre de 2003,

bajo un nuevo concepto de seguridad hemisférica que amplía la definición tradicional de la defensa y seguridad de los Estados, a partir de la incorporación de nuevas amenazas, preocupaciones y desafíos, y que incluyen aspectos políticos, económicos, sociales, de salud y ambientales. De este modo, casi todos los problemas pueden ser considerados una potencial amenaza a la seguridad (Chiller & Freeman, 2005).

A partir de la creación de la Secretaría de Seguridad Multidimensional (SSM), se estableció el concepto multidimensional de la seguridad como un principio fundamental de la seguridad para la protección de los seres humanos. Esta declaración representa un gran avance en el reconocimiento de carácter multidimensional a los conflictos que se plantean en el campo de la seguridad hemisférica. También se la considera un significativo esfuerzo por enfrentar las amenazas atendiendo también sus causas (Chiller & Freeman, 2005).

En consecuencia con lo anterior, desde finales del siglo XX, las Naciones Unidas ajustaron su propia organización para dar respuesta a todas las amenazas que afectan a los seres humanos; desafortunadamente, las medidas adoptadas por la Organización de las Naciones Unidas (ONU) en temas de seguridad global, seguridad y desarrollo humano no fueron replicadas ni adoptadas en todas partes. En el hemisferio americano, a pesar de las circunstancias económicas del mundo, una más que considerable región en vía de desarrollo aún busca, de alguna manera, adoptar la mayoría de los compromisos adquiridos a través de la OEA. Las acciones de confianza no son suficientes si la política de lucha contra las nuevas amenazas a la seguridad multidimensional no se adoptan en común.

Ahora bien, el Estado colombiano, por su ubicación geoestratégica en el continente, enfrenta grandes retos en la lucha contra la criminalidad, además de los riesgos inherentes a su integridad territorial, por las amenazas que provienen de naciones cercanas con aspiraciones territoriales, soportadas en profundas diferencias ideológicas, como la inestabilidad de sus fronteras, lo que obliga a mantener una permanente vigilancia de los acontecimientos externos.

De este modo, contemplar el empleo del poder aéreo, espacial y ciberespacial en ambientes particulares o multidominio, sobre la base de la supervivencia del Estado en contribución al desarrollo y la prosperidad nacionales, permite demostrar cómo desde estos dominios es más eficaz combatir las amenazas multidimensionales que enfrenta la nación, bajo la premisa de que dichos poderes no son de exclusiva aplicación para fines militares. Por el contrario, contemplarlos

bajo una condición estratégica multidominio, y emplear sus capacidades de forma integral en esfuerzos de acción unificada (AU), permite obtener grandes resultados en función de la seguridad y defensa para la protección de los intereses nacionales.

En este sentido, la investigación planteó como objetivo general *Establecer la proyección de empleo del poder aéreo, espacial y ciberespacial para combatir y contener las amenazas con los nuevos desafíos multidimensionales que enfrenta el Estado colombiano para garantizar la seguridad y defensa nacional*.

A fin de lograr dicho objetivo, el grupo de investigadores estableció una ruta metodológica, partiendo de tres objetivos específicos, los cuales facilitaron el análisis de los hallazgos y, la concreción de los argumentos planteados en los cinco capítulos que componen el presente libro:

- Examinar el ambiente global y regional de amenazas multidimensionales que afectan la seguridad y defensa nacional.
- Identificar las amenazas, los nuevos retos y los desafíos multidimensionales que enfrenta la nación colombiana.
- Determinar cómo el poder aéreo, espacial y ciberespacial contribuye a combatir y contener las amenazas y los nuevos desafíos multidimensionales que afectan al Estado colombiano.

De este modo, el primer capítulo denominado *Pasado, presente y futuro: impacto de las nuevas amenazas en el rol de la Fuerza Aérea Colombiana en los tiempos de la seguridad multidimensional* esboza inicialmente, desde el nuevo enfoque de seguridad, el desarrollo de nuevas estrategias de los Estados; especialmente, con el empleo de las Fuerzas Armadas (FF. AA.), antes encaminadas a la integralidad del territorio nacional y a la protección de las fronteras, y ahora, asumiendo nuevos roles que en otros tiempos habrían sido competencia de otras instituciones. A continuación, en el capítulo se presenta a la Fuerza Aérea Colombiana (FAC), líder del poder aéreo nacional, como una institución militar que, en la búsqueda de la superioridad en el aire y el dominio de la soberanía del país en los cielos, adelantó un riguroso proceso de modernización y transformación a través del tiempo, motivada, en parte, por las circunstancias operacionales propias del conflicto armado colombiano.

Posteriormente, se hace un análisis del impacto de las nuevas amenazas que afectan al Estado colombiano, y de cuál ha sido la contribución, desde las capacidades misionales de la FAC, a la seguridad multidimensional del país; se plantearon, igualmente, algunas reflexiones, sobre la base de temáticas relacionadas

con: el paso de la concepción de seguridad nacional a la de seguridad multidimensional en el país, así como sobre el rol de las Fuerzas Militares de Colombia (FF. MM.), mediante un sucinto recuento histórico del papel de la FAC, en los tiempos de la *seguridad nacional* y en los de la *seguridad multidimensional* y, por último, sobre las capacidades de la FAC en relación con las nuevas amenazas. El capítulo aporta desde la academia un insumo más, que permita a los tomadores de decisiones entender cómo se ha desenvuelto la FAC en esta transición, y algunas recomendaciones en la aplicación de estrategias, que posibiliten un mejor acoplamiento de las exigencias del mundo moderno con respecto a las actividades de esta fuerza militar y del aire.

El segundo capítulo, titulado *Contexto global contemporáneo de cara a las amenazas, nuevos retos y desafíos multidimensionales,* aborda, desde el marco de la seguridad, el orden mundial y las relaciones internacionales, fundamentos para entender la evolución de las amenazas tradicionales y las nuevas amenazas que enfrentan los Estados. Se analizan algunos eventos que han generado cambios en el ambiente internacional a lo largo del siglo XXI, los cuales llevan a consolidar de forma prioritaria el concepto *seguridad nacional*, así como el concepto *defensa colectiva*. También se presenta una categorización de las nuevas amenazas de mayor impacto que afectan el mundo contemporáneo, a partir de la Declaración de la Seguridad de las Américas del 2003 de la Organización de los Estados Americanos (OEA) —lo cual, a su vez, permite hacer un análisis comparativo con otras organizaciones, como la Organización del Tratado del Atlántico Norte (OTAN), la ONU y la Oficina de las Naciones Unidas contra la Droga y el Delito (en inglés, UNODC, por las iniciales de United Nations Office on Drugs and Crime)—. A raíz de dicha categorización, se hace visible la mutación de esas nuevas amenazas que trascienden las fronteras.

Acto seguido, se presenta una evaluación de los sucesos de mayor relevancia del siglo XX y del siglo XXI que han generado un cambio en el orden mundial en el área de las relaciones internacionales y las nuevas amenazas del mundo contemporáneo, lo que permite, a su vez, proponer los posibles retos del mundo en el marco de la seguridad para las próximas décadas. Este último es un aspecto pertinente a desarrollar análisis prospectivos de las estrategias de seguridad de los Estados para combatir los futuros peligros que empiezan a gestarse en el ambiente ciberespacial.

El tercer capítulo muestra, como lo indica su título, las *Capacidades del Estado colombiano para combatir las amenazas y los desafíos multidimensionales en*

los dominios aéreo y ciberespacial, a partir de la caracterización de las nuevas amenazas transnacionales generadas por actores estatales y organizaciones no estatales, y que afectan la seguridad de los Estados y dificultan contenerlas o combatirlas. 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, que le permitan emplear sus capacidades para enfrentarlas y visualizar nuevos desafíos.

Las nuevas amenazas que afectan a los Estados aprovechan el ciberespacio con la particularidad del "anonimato", en muchos casos. Dichas ciberamenazas se potencializan por la masificación en el uso de tecnologías de la información que emplean internet y las redes informáticas para generar ciberataques; principalmente, a la infraestructura crítica. Las FF. MM. hacen parte de las capacidades de seguridad y defensa del Estado, mediante la ciberdefensa, a fin de preservar los intereses nacionales.

La FAC, en medio de su evolución hacia una doctrina del poder multidominio, involucra el aire, el espacio y el ciberespacio como dominios para realizar sus operaciones. De este modo, a la FAC se la considera un actor fundamental en la estrategia de seguridad multidimensional para enfrentar las amenazas y preservar el interés nacional. En tal sentido, surge la hipótesis de que *los intereses del Estado pueden verse afectados con la materialización de las amenazas en los dominios aéreo y ciberespacial*, por lo cual determinar el impacto de dicha afectación permite plantear estrategias para combatirlas y contenerlas.

El cuarto capítulo, titulado *Amenazas y desafíos multidimensionales para la ciberseguridad y la ciberdefensa, en los dominios espacial y ciberespacial*, presenta reflexiones sobre el desarrollo del dominio espacial colombiano como una futura capacidad autónoma y sostenible, a pesar de las limitaciones del Estado en la explotación de dicho interés nacional. A partir de la puesta en órbita, por parte de la FAC, del satélite FACSAT-1 para la observación de la Tierra, se genera un nuevo campo de desarrollo sobre el ámbito espacial en el país.

Acto seguido, se plantean algunas reflexiones sobre cómo diversas organizaciones a escala nacional poseen y operan estaciones terrestres, por lo cual obtienen el acceso a productos y servicios de proveedores externos, como las comunicaciones y las imágenes, para propósitos meteorológicos o de análisis de terreno y control de tráfico aéreo. Sistemas de información que requieren protección contra las amenazas cibernéticas asegurando la disponibilidad permanente, la integridad y la confidencialidad, y evitando degradar la

confiabilidad en el desempeño de los sistemas y los activos estratégicos del ámbito espacial.

El capítulo, con respecto al dominio ciberespacial, hace referencia a lo indispensable que es reconocer el papel que desempeña dicho dominio en la transformación del mundo, suscitada por la Revolución Industrial 4.0: la era de la digitalización y la masificación de tecnologías en todos los sectores, los modelos de negocios y las cadenas productivas. Una condición que no ha pasado desapercibida en la transformación del sector público, la seguridad nacional y, por supuesto, las amenazas asociadas en un mundo cada vez más globalizado e interconectado a través del procesamiento de la información transitando por el ciberespacio.

Al cierre, el capítulo plantea la existencia de diferentes factores de inestabilidad sobre el dominio espacial identificando la necesidad de un interés nacional permanentemente para mantener la nación protegida de los riesgos asociados a esos dominios, y su estrecho vínculo con el funcionamiento de la infraestructura crítica.

El quinto capítulo, denominado *Poder multidominio: visión estratégica de la Fuerza Aérea Colombiana en el siglo XXI*, expone cómo el espacio exterior y el ciberespacio se han convertido en nuevos campos de batalla altamente competidos y congestionados, donde se generan efectos a la velocidad de la luz. Esta disruptiva ampliación de los campos de batalla hace que el combate se traslade a través de los dominios, y sea conducido a una velocidad y con un alcance incrementales, desde el escenario táctico del combate cercano, atravesando teatros internacionales y alcanzando, incluso, el interior de un país.

Por otra parte, el capítulo hace énfasis en lo que se considera la avalancha mundial de una tecnología comercial poderosa y fácilmente disponible, y la cual exige un enfoque mucho más sofisticado para los asuntos militares generando un entorno de seguridad donde el ritmo del avance cibernético, de energía dirigida, nanotecnología, robótica y biotecnología va mucho más allá de la capacidad normal para predecir sus efectos. Una condición que motiva a los Estados a revisar sus propias dinámicas de seguridad y defensa, y a desarrollar nuevas estrategias que lleven al logro de sus intereses nacionales.

De forma complementaria, se describe a los actores estatales y no estatales que usan otros recursos adicionales para imponerse a sus adversarios incrementado su propia capacidad apoyados en la era de la información, lo que les permite ahora tener alcance global y masivo. Es el caso de la guerra de la

información, y de las operaciones ambiguas, o de negación de poder, y de la subversión (Álvarez & Jiménez, 2021). Panorama que avizora cómo las estrategias de seguridad y defensa de los Estados también se transforman respondiendo con la adopción de cambios estratégicos, como el fortalecimiento de las relaciones, e involucrando socios que proveen oportunidades para la cooperación (organizaciones multilaterales, organizaciones no gubernamentales [ONG], corporaciones, influenciadores estratégicos y asociaciones); y cambios que impactan el nivel operacional, como la incorporación y el uso de las tecnologías emergentes, que incluyen la computación avanzada.

Finalmente, y en procura de adaptarse al nuevo campo de batalla multidominio, surge la necesidad, para la FAC, de adoptar una visión de *poder multidominio*, que provea una mejor consciencia situacional, al igual que la rápida toma de decisiones, por parte del comandante, así como el ágil despliegue de capacidades en los dominios de aire, espacio y ciberespacio, a través de un Comando y Control Multidominio (MDC2), y de tal manera que la FAC pueda adaptarse rápidamente a las amenazas y las oportunidades, y crear efectos a través de los dominios aéreos, espaciales y ciberespaciales, en el tiempo y el lugar necesarios y mediante el método escogido.

A modo de conclusión, los capítulos presentan las consideraciones finales resultado de los hallazgos más importantes de la investigación, dando cuenta, a su vez, del logro de los objetivos específicos del proyecto, a fin de, demostrar cómo el empleo del poder aéreo, espacial y ciberespacial, en ambientes particulares o multidominio, son más eficaces para combatir las amenazas multidimensionales que enfrenta la nación, toda vez que, al aplicarlos bajo una condición estratégica multidominio, mediante el empleo de capacidades de forma integral, permiten obtener grandes resultados en función de la seguridad y defensa en la protección de los intereses nacionales.

Referencias

Álvarez, C., & Jiménez, H. (2021). Guerra de información y ética militar: entre la tradición de guerra justa y la teoría de guerra irrestricta. En J. Jiménez, C. Figueroa, & M. Bricknell (Eds.), *Ética militar y fuerza pública en Colombia* (Vol. II, pp. 71-111). Sello editorial ESMIC.

Chillier, G., & Freeman, L. (2005). *El nuevo concepto de seguridad hemisférica de la OEA: Una amenaza en potencia.* https://tinyurl.com/4v77vzak

Organización de Estados Americanos (OEA). (2011, 5 de junio). *La Seguridad Multidimensional y los retos actuales*. José Miguel Insulza, Secretario General. XLI Asamblea General de la OEA, San Salvador. https://tinyurl.com/4tazfay8

Capítulo 1

Pasado y futuro: Nuevas amenazas y el rol de la FAC en tiempos de seguridad multidimensional*

DOI: https://doi.org/10.25062/9786287602106.01

Gustavo Adolfo Ocampo Nahar
Tito Saúl Pinilla Pinilla
Martha Beatriz Tovar Zambrano
Juan David Mora Peña
Escuela de Altos Estudios Estratégicos Nueva Granada

Resumen: Este capítulo tiene por objeto analizar el impacto de las nuevas amenazas y la contribución desde las capacidades de la Fuerza Aérea Colombiana (FAC) en las áreas misionales de la seguridad multidimensional del país. Para ello, se abordan las siguientes temáticas: el origen de la concepción de la seguridad nacional en Colombia; el paso de la seguridad nacional a la seguridad multidimensional; el rol de las Fuerzas Militares en Colombia (FF. MM.), y para finalizar, un recuento histórico del rol de la FAC durante los tiempos de la seguridad nacional y la seguridad multidimensional.

Palabras clave: FAC, defensa, nuevas amenazas, seguridad multidimensional, seguridad nacional.

* Capítulo de libro elaborado por Escuela de Altos Estudios Estratégicos Nueva Granada 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.

Gustavo Adolfo Ocampo Nahar
Mayor General de la Reserva Activa de la Fuerza Aérea Colombiana, del Cuerpo de Seguridad y Defensa de Bases Aéreas y Administrador Aeronáutico. Magíster en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto ESDEG. Director del Escuela de Altos Estudios Estratégicos Nueva Granada de la UMNG. - Contacto: gustavo.ocampo@unimilitar.edu.co

Tito Saúl Pinilla Pinilla
General de la Reserva Activa de la Fuerza Aérea Colombiana, Piloto militar y administrador aeronáutico. Magíster en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto", ESDEG. Asesor en la Escuela de Altos Estudios Estratégicos Nueva Granada, líder de la línea de investigación de Narcotráfico en la UMNG.

Martha Beatriz Tovar Zambrano
PhD en Administración de la Universidad de Celaya, México, Magíster en Educación de la UMNG. Egresada del Curso Integral de Defensa Nacional (CIDENAL), en la Escuela Superior de Guerra "General Rafael Reyes Prieto", ESDEG. Administradora de Empresas. Investigadora en la Escuela de Altos Estudios Estratégicos Nueva Granada, Universidad Militar Nueva Granada, líder de la línea de investigación de Estudios Antárticos. Orcid: https://orcid.org/0000-0002-6036-0898 - Contacto: martha.tovar@unimilitar.edu.co

Juan David Mora Peña
Magíster en Estrategia y Geopolítica de la Escuela Superior de Guerra "General Rafael Reyes Prieto", Especialista en Estudios Políticos de la Universidad Sergio Arboleda y Abogado de la Pontificia Universidad Javeriana. Investigador de la Escuela de Altos Estudios Estratégicos Nueva Granada Universidad Militar Nueva Granada, en la línea de Narcotráfico. Orcid: https://orcid.org/0000-0002-2952-9608 - Contacto: juand.mora@unimilitar.edu.co

Citación APA: Ocampo Nahar, G. A., Pinilla Pinilla, T. S., Tovar Zambrano, M. B., & Mora Peña, J. D. (2022). Pasado, presente y futuro: impacto de las nuevas amenazas en el rol de la Fuerza Aérea Colombiana en los tiempos de la seguridad multidimensional. En F. Baquero Valdés (Ed.), *Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano* (pp. 21-61). https://doi.org/10.25062/9786287602106.01

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

Con el desarrollo de un mundo alejado de la bipolaridad surgida durante la Guerra Fría, las amenazas a la seguridad de las naciones han mutado enormemente. Sin el miedo a la destrucción masiva asegurada, la comunidad internacional ha hecho un giro en sus acercamientos a los retos que viven los Estados modernos, y se ha enfocado radicalmente en el bienestar del ser humano por sobre el del Estado. De esa manera, han surgido nuevos enfoques en referencia a la seguridad, y que se alejan del clásico modelo de la seguridad nacional, que había sido utilizado a lo largo del tiempo; en particular, a lo largo de la segunda mitad del siglo XX.

En consecuencia, empiezan a surgir, desde la voluntad de los mismos Estados y de las organizaciones internacionales, enfoques como la *seguridad humana*, descrita en el Informe de Desarrollo Humano de la Organización de las Naciones Unidas (ONU) de 1994. En lo regional, la Organización de Estados Americanos (OEA), en busca de un cambio radical del enfoque de seguridad que había sido utilizado en la región durante la Guerra Fría y las dictaduras militares y civiles del siglo XX, originó el concepto *seguridad multidimensional*, caracterizada por una amplia descripción de amenazas que han impuesto la obligación a los Estados de proteger a la ciudadanía de peligros como la degradación medioambiental, las crisis económicas que llevan a la pobreza extrema, la precariedad laboral y la seguridad ciudadana, entre otras.

Este enfoque de seguridad ha generado un impacto en el desarrollo de las actividades de los Estados y su aparato administrativo; especialmente, en las

funciones de las Fuerzas Armadas (FF. AA.) de cada país, antes encaminadas a la integralidad del territorio nacional y a la protección de las fronteras, y ahora, teniendo que asumir roles que en otros tiempos habrían sido competencia de otras instituciones.

Ahora bien, en ese modelo resulta de gran relevancia destacar el papel de la (FAC). Su labor, dedicada al desarrollo del poder aéreo nacional, la búsqueda de la superioridad en el aire y la soberanía del país en los cielos se ha transformado a través del tiempo. Durante el conflicto armado, la FAC pasó a ser un arma contrainsurgente que, gracias a sus aviones tácticos, como los Super Tucano, los Dragonfly o los Kfir, han asestado fuertes golpes a los grupos armados al margen de la ley, como las Fuerzas Armadas Revolucionarias de Colombia (FARC), el Ejército de Liberación Nacional (ELN) y los paramilitares, al igual que a los nuevos grupos, como las disidencias de las FARC, El Clan del Golfo y Los Rastrojos. No obstante, con la entrada del nuevo enfoque de la seguridad multidimensional, la FAC ha contribuido al desarrollo de nuevas actividades fuera de su gestión tradicional; entre estas, la ciberseguridad, el apoyo para la protección del medioambiente y la acción integral.

El propósito del presente capítulo es analizar el impacto de las nuevas amenazas y la contribución desde las capacidades de la FAC a las áreas misionales en la seguridad multidimensional del país, para lo cual se abordarán las siguientes temáticas: el paso de la concepción de seguridad nacional a la seguridad multidimensional en el país; el rol de las FF. MM. de Colombia; un recuento histórico sobre el papel de la FAC durante los tiempos de la seguridad nacional y la seguridad multidimensional, y por último, las capacidades de la FAC en relación con las nuevas amenazas. Lo anterior busca aportar desde la academia un insumo que permita a los tomadores de decisiones entender cómo se ha desenvuelto la FAC en esta transición, y algunas recomendaciones para realizar estrategias que posibiliten un mejor acoplamiento de las exigencias del mundo moderno con respecto a las actividades de la Fuerza.

El origen de la concepción de la seguridad nacional en Colombia

Para iniciar este apartado es importante tomar en cuenta qué define el concepto *seguridad*, del que se hará reiterado uso a lo largo del texto. Para este caso, se hará referencia a Ugarte (2001), quien hace un análisis del concepto de la

seguridad desde las amenazas, y deja claro que la seguridad busca evitar los daños que las amenazas puedan ocasionar. Es comprensible que tal afirmación resulte, de alguna manera, simple; no obstante, el autor logra demostrar que esta sencilla definición aplica para todo tipo de seguridad: la seguridad social, la seguridad económica, la seguridad jurídica y, claro está, la seguridad nacional. De esa manera, cuando se hace referencia en el presente texto a *seguridad nacional*, se la debe entender como

> El objetivo de prevenir o rechazar amenazas militares y, por tanto, defender militarmente la soberanía, la independencia y la territorialidad del Estado frente a posibles agresores. De esta manera, el Estado busca su propia seguridad incrementando su poder a través de su capacidad militar. (Font & Ortega, 2012, p. 161)

Una definición que con el tiempo ha ido cambiando radicalmente, pero que en un mundo que ha funcionado a partir del ejercicio del poder y del realismo debe tenerse en cuenta como principal eje de las relaciones internacionales. Como se verá a continuación, la concepción y el ejercicio de la seguridad nacional en Colombia han variado, al pasarse de un enfoque que replica las amenazas descritas en la teoría realista de las relaciones internacionales —en este caso, las tradicionales— a otro que logra dar ingreso a amenazas a las que antes no se consideraba de competencia del Estado, ni, por tanto, de sus FF. AA., pero ahora involucradas estas últimas en un gran número de funciones que antes era impensable atribuirles. Así, seguidamente se muestra de manera detallada esta evolución y su impacto en el ejercicio de la seguridad en el país.

Desde los primeros días de la consolidación del Estado nación, el ejercicio del poder se ha truncado por cuenta de numerosos acontecimientos que han llevado al quebrantamiento del poder nacional en amplias áreas periféricas de la geografía territorial. Lo anterior se ve reflejado en las múltiples confrontaciones fratricidas entre colombianos, que se han visto durante los siglos XIX, XX y XXI, y que han ocasionado, en gran medida, y con sus dinámicas específicas, que en amplios territorios del país se dispute al Estado colombiano su legítimo uso de la fuerza, y a que sea imposible, en consecuencia, instituir políticas públicas en pro de la reconstrucción del tejido social desarraigado por la violencia. Lo anterior ha transformado el desarrollo de políticas de seguridad, que se han enmarcado en la lucha contrainsurgente, y no en la guerra de tipo convencional, como en otras regiones del mundo y en Latinoamérica.

Con este escenario planteado, resulta claro que en Colombia se ejerció un sistema de políticas en seguridad que difería de la idea de otros países latinoamericanos, más enfocados en la lucha contra sus vecinos que en la del control del orden interno. El Estado nación colombiano, fraccionado en una gran variedad de espacios geográficos estratégicos, se vio impedido durante el siglo XIX para unificar el sistema de gobierno nacional, y hasta atrayendo conflictos políticos entre las regiones.

El primer hito concerniente a las disposiciones de seguridad en el país fue la guerra civil acaecida durante la época de la mal llamada Patria Boba. Durante dicho conflicto bélico se estructurarían, por primera vez, tendencias que se mantuvieron constantes: la fragmentación del espacio geográfico en diferentes centros de poder, la incapacidad del Gobierno central para cooptar el uso de la fuerza y la irrupción de la afectación del orden público nacional. Así, con posterioridad a las diversas declaraciones de independencia de territorios inmersos en el antiguo Virreinato de la Nueva Granada —especialmente, en ciudades como Santafé, Cartagena de Indias y Tunja—, se presenció un quiebre entre los gobernantes que buscaban mantener el ejercicio del poder nacional, y se presentó, de esta manera, la pugna entre dos sistemas de gobierno que se encontraban en boga durante aquel tiempo (Bushnell, 1996).

En primer lugar, la ciudad de Santafé, autodenominada estado de Cundinamarca en su declaración de independencia absoluta, del 16 de julio de 1813, con fuerte carácter centralista y al mando del general Antonio Nariño. En segundo lugar, las Provincias Unidas de la Nueva Granada, consolidadas desde el 27 de noviembre de 1811 y encabezadas por Cartagena de Indias y Tunja. Fue durante esa época de pugna ideológica e instrumental cuando empezaron a estructurarse las primeras milicias independientes de la corona española. De acuerdo con Pardo (2008),

> […] la primera actividad militar de la nueva Junta de Gobierno de Santafé fue tratar de organizar una fuerza armada, por lo que dispuso la creación de un batallón de voluntarios de la Guardia Nacional, cuya formación fue anunciada a la ciudadanía en un bando emitido el 23 de julio de 1810, pero que en realidad no se constituyó como tal hasta noviembre de ese año. […] Se organizaron unas milicias que se denominaron Patriotas de Defensa, para prestar seguridad en la capital. (pp. 99-100)

Sin embargo, independientemente de los esfuerzos de personajes como Antonio Nariño, Francisco José de Caldas y Camilo Torres, los generales del

momento nunca tuvieron la capacidad ni el entrenamiento para el ejercicio de la carrera militar. De esta forma, según Deas (2017), ninguno de dichos personajes es recordado por sus acciones militares, sino, más bien, por sus labores de construcción de las primeras bases del sistema político y jurídico de Colombia. Solo con la llegada de las tropas del general Pablo Morillo y la reconquista, fue como las esperanzas de los cabildos surgidos durante la primera generación del siglo XIX terminarían.

Posteriormente, generales oriundos de la Capitanía de Venezuela y de la Nueva Granada iniciaron la reestructuración del sistema militar patriota (Bushnell, 1996). Así, en Casanare, mientras se hallaba alejado de los centros de poder realistas donde se encontraba el reinstituido virreinato español, el general Francisco de Paula Santander estableció el primer nicho del actual sistema militar colombiano.

Para finales de la guerra de Independencia, y tras la consolidación del territorio de la Capitanía de Quito y la liberación del Alto Perú y del Bajo Perú, el sistema militar de la República de Colombia, liderado en lo militar por el general Simón Bolívar, y en lo administrativo, por el general Santander, había pasado de tener un pie de fuerza de 7.000 efectivos en 1819, a 23.000, en 1823 (Pardo, 2008).

Fue a partir de ahí cuando la República de Colombia consolidó sus propias fronteras, elemento primordial para la formulación de una estrategia de seguridad. El territorio nacional se compondría de las posesiones del Virreinato de la Nueva Granada: es decir, los territorios de Colombia, Panamá, Ecuador y Venezuela, y algunos puntos de la costa de Mosquitos, que se introducía en predios de las actuales Costa Rica y Nicaragua; de ahí que el posicionamiento estratégico de la nueva nación encontrase en su carácter bioceánico un insumo geoestratégico de gran magnitud. De acuerdo con Afanador-Llach (2018), la geografía se convirtió en un elemento de unión nacional que buscaba, en el imaginario, terminar con las separaciones regionalistas que abundaban en el lugar, pero que poco a poco fueron desmembrando el gran sueño americano. Estos elementos entregados por la nueva geografía de la Gran Colombia significaron un desafío de gran magnitud en cuanto a la defensa de la nueva nación; sin embargo, esta debía ser resguardada por un pequeño Ejército Nacional muy fragmentado.

Quito, Caracas, Bogotá y Panamá fueron llamadas a consolidarse como posiciones estratégicas que garantizarían la seguridad ante amenazas por parte de intereses extranjeros; entre ellas, la de los españoles, que aún mantenían su

pretensión de un proceso de reconquista. Pero debido a su situación interna, la novel nación no había podido desarrollar de manera correcta dicho afianzamiento. Aquello solo sería finiquitado en 1820, con el pronunciamiento de Riego, quien debía apoyar los esfuerzos realistas de Morillo en territorio neogranadino.

Con el tiempo, la gran separación geográfica de los territorios del nuevo país, los intereses particulares de los terratenientes en amasar poder y la reticencia por parte de Santafé a aumentar la autonomía regional llevaron a la lucha entre regiones, lo que derivó en el desmembramiento de la Gran Colombia, en 1831. Fue a partir de ese momento cuando el ejército que había independizado América se vio reducido a un pequeño contingente, casi nulo. Para Esquivel (2010),

> La historiografía es reiterativa, sin profundizar al respecto, sobre que desde 1830 se redujo al mínimo el ejército permanente, y su incremento fue episódico según las necesidades de los conflictos internos; incluso, se asume que en la práctica entre 1830 y 1886 no hubo Ejército Nacional. (p. 161)

Con ello, la seguridad internacional e interna quedaba expuesta ante cualquier amenaza tradicional; es decir, la concepción de seguridad nacional era nula ante los graves problemas que vivía el país. Asimismo, Deas (2017) expone que las causales de dicha reducción, casi absoluta, del poder militar de Colombia fueron consecuencia de la fuerte carga fiscal que conllevaba mantener al ejército que había liberado el territorio nacional. Con ello, no fue extraño que, para los gobiernos posteriores a la separación de la Gran Colombia, el ejército solo tuviera relevancia en momentos de gran caos interno, en el que se viera muy amenazado el poder central. Igualmente, no se consideraba necesario un ejército demasiado grande para la defensa de puntos clave de la geografía nacional; entre ellos, Cartagena de Indias, Santafé y el acceso al río Magdalena, entre otros. Y en tercer y último lugar, cabe tener en cuenta la prevalencia en su política exterior del derecho como máxima forma de defensa territorial del país frente a otras naciones, y el consecuente abandono de su capacidad militar.

Con lo planteado, se hace evidente que la concepción de seguridad sería muy alejada de otras ideas de seguridad en los ámbitos regional y mundial. La geografía impidió la unión entre los centros de poder en el país, y se generó, pues, una tensión entre el centro y las regiones, lo que, a su vez, llevó a múltiples escenarios de caos interno entre ejércitos independientes. Así, el establecimiento de un sistema federal por parte de los liberales cerraba aún más las puertas a la posibilidad de consolidar un sentimiento nacional, e incrementaba las discusiones entre los diferentes estados de Colombia. No será poco común encontrar

guerras abiertas entre estados a los que Santafé, ahora Bogotá, no podría acceder con su nula capacidad militar.

De esta manera, la defensa de la soberanía fronteriza pasó a un segundo plano, y debilitó en gran medida la capacidad de defensa nacional. Esquivel (2010) dice que

> La historiografía refiere anecdóticamente que Colombia sufrió, entre otras, la invasión de tropas peruanas (1829, 1911), ecuatorianas (1832, 1839, 1863, 1900), venezolanas (1845, 1847, 1855, 1901), nicaragüenses (1901), el dominio inglés sobre la costa de Mosquitia (desde 1847), el bloqueo marítimo y el bombardeo por flotas armadas francesas (1833), inglesas (1836, 1856) e italianas (1885, 1898) y la presión naval alemana (1870), sin olvidar las no todas solicitadas catorce intervenciones estadounidenses en Panamá (1855 a 1903). (p. 158)

Y es que a lo largo del siglo XIX hubo importantes conflictos civiles entre conservadores y liberales, herederos de las pugnas entre bolivarianos y santanderistas, por el posicionamiento político, cultural, religioso e, incluso, educativo de la nueva nación. Con ello, se presentaron cuatro grandes guerras civiles que redujeron la casi nula idea de seguridad a un carácter interno. De tal manera, durante la hegemonía radical de los liberales, la Fuerza Pública —especialmente, el Ejército— sería una simple guardia civil, conocida como Guardia Nacional, y pequeños ejércitos estatales, bajo el control de grandes terratenientes regionales (Atehortúa & Vélez, 1994).

Solo hasta 1886 la idea de seguridad empezó a estar ligada al sentimiento nacional. Anteriormente, como se ha mostrado, la división territorial e ideológica no permitió la existencia de una nación consolidada como tal, sino la de un Estado. Con ello, el objetivo del presidente Rafael Núñez —antiguo liberal, y ahora, férreo defensor de las ideas conservadoras— era la consolidación territorial mediante el advenimiento de un sentimiento nacional. Así, "la contribución de Núñez a la causa de la unificación nacional no consistió exclusivamente en la redacción de una nueva Constitución que reforzaba el ejecutivo nacional […]. También fue simbólica, al dar a sus compatriotas un Himno Nacional" (Bushnell, 1996, p. 199); hizo lo mismo en cuanto a las ideas religiosas, económicas, productivas, industriales y militares.

Con la llegada de la Constitución de 1886, se buscó y se justificó la concentración del monopolio de la fuerza en un solo poder —el Ejército Nacional—, y la soberanía nacional fue clave para un verdadero ejercicio de la seguridad

nacional. Para Núñez, el ejercicio de la seguridad del Estado se basaba en la capacidad para el manejo de la fuerza y en la centralización del elemento nacional. De acuerdo con Rosanía et al. (2017), aquella transformación de Rafael Núñez llamaba la Regeneración Nacional, ante un sistema federalista y liberal disruptivo de la construcción de una unidad nacional, permitió que se aglomerase en un solo sentimiento de identidad a la población del país, y permitió al presidente posicionarse como comandante en jefe de todas las FF. AA. del país. Con eso, y más allá de una simple reforma política, la Regeneración significó la retoma del poder político del centro sobre las periferias y los centros de poder a lo largo y ancho del país.

Evidentemente, esa transformación política, social y económica de la nación colombiana no vino sin contratiempos. Desde el inicio de la Constitución de 1886, aquellos proscritos de la política, pero con suficiente poder económico —especialmente, en las regiones—, buscaron por medio de las armas luchar contra el poder centralizado de Bogotá. Lo anterior obligó, de manera imperativa, a la consolidación de un Ejército Nacional, protagonista de las cruentas guerras civiles que se presentarían durante los últimos años del siglo XIX. El objetivo, como tal, más allá de luchar contra quienes desearan atentar contra el orden constitucional, fue recuperar un elemento principal en la estructuración de los Estados modernos: el monopolio de la fuerza; también, establecer un pensamiento de seguridad más cercano a lo establecido por la escuela realista de las relaciones internacionales. Sin embargo, como ya se ha dicho, se mantuvo la prioridad por el orden nacional.

Fue con la separación de Panamá y el fin de la guerra de los Mil Días cuando Colombia buscó, por primera vez, la profesionalización de su Ejército Nacional. Así, en 1909 se instituyó la Escuela Superior de Guerra (ESDEG), junto con otras escuelas de formación militar, en las que se daría una educación profesional a los oficiales que las integren. Con ello, se inició la profesionalización, de la mano con el Ejército de Chile, que había salido vencedor durante la guerra del Salitre, o guerra del Pacífico, contra sus vecinos de Perú y Bolivia. El Ejército de Chile había logrado incorporar la tecnología europea —especialmente, la prusiana— en su doctrina bélica, lo que aportaría a Colombia una imagen de lo que se venía desarrollando doctrinal y tecnológicamente en Europa (Rodríguez, 2006).

Es así como el Estado colombiano, gracias, en parte, a las capacidades de reconstrucción del estamento militar de los presidentes Núñez y Reyes, logró estabilizar sus fronteras. En las primeras décadas del siglo XX, a pesar de los

pequeños esfuerzos por modernizarse, el Ejército no tuvo la capacidad para hacerlo. Su profesionalización evolucionó; sin embargo, los esfuerzos no se vieron recompensados. De acuerdo con Deas (2017), entre los mayores problemas que se presentaron durante la época estuvo la constante animadversión antimilitarista que profesaron los políticos colombianos desde el siglo XIX. De esta manera,

> El Ejército continuó siendo modesto. Tuvo su utilidad, no fue enteramente descuidado, y evolucionó poco a poco […]. El pequeño cuerpo de oficiales siguió estando compuesto en su mayoría de conservadores, y si bien no se ha hecho ningún estudio sistemático, hay indicios de que un ancestro conservador fue característico de sus miembros hasta los años sesenta, aunque su filiación partidaria no era del todo de la misma naturaleza de la que marcaba a los políticos. (p. 35)

Claro está, a pesar de mantener un Ejército reducido, las FF. AA. se empezaron a consolidar como elemento básico del poder del Estado y, por tanto, como un elemento clave para el ejercicio de la soberanía (Rosanía et al., 2017) y de la implementación de una rudimentaria seguridad nacional. De igual manera, desde la visión de las relaciones internacionales, Colombia comenzó a establecer una atenta mirada sobre sus propias fronteras —especialmente, en el Caribe y en el Amazonas—, y a concretar, también por primera vez, fronteras anteriormente difíciles de comprender. Asimismo, fue durante esa época cuando se firmaron tratados como el Esguerra-Bárcenas, en 1928, con Nicaragua; Vélez-Victoria, con Panamá, en 1924; Lozano-Salomón, con Perú, en 1922, y Suárez-Muñoz, con Ecuador, en 1916, así como el Acta Tripartita de Límites y Navegación entre Colombia, Perú y Brasil, en 1925, etc., que dieron un auge al proceso de demarcación territorial que durante el siglo XIX no había sido posible.

Con el tiempo, en las primeras décadas del siglo XX, el Ejército y el concepto de seguridad estuvieron reducidos. No obstante, y a pesar de una importante disminución en la violencia partidista producida durante el siglo XIX, en Colombia se mantuvo el sistema de seguridad que garantizaba la consolidación del orden interno; especialmente, en las zonas periféricas.

Sin embargo, los radicales cambios políticos que vivió el país durante la década de 1930, con la llegada de la hegemonía liberal —tras largo tiempo viéndose apartados los miembros de dicho partido del actuar de la política—, desembocaron en un nuevo proceso de violencia. Durante el decenio de 1940 se generó una dinámica que en la historiografía nacional ha sido establecida como La Violencia

(1946-1965), la cual partió la sociedad en sectores partidistas —sobre todo, en las regiones más periféricas—, y en nombre de la cual se produjeron grandes masacres entre simpatizantes de uno u otro partido. Lo anterior terminó por debilitar el concepto de seguridad.

Las FF. AA. —en especial, el Ejército y la Policía— ingresaron en esa dicotomía, y se vieron obligadas a establecer un férreo ejercicio del orden interno. Lo anterior, generado, en gran medida, por un sentimiento antimilitarista de la sociedad política; sobre todo, la liberal, proclive a un gobierno de carácter marcadamente progresista, encabezado por el presidente Alfonso López Pumarejo, y por la desincentivación de los esfuerzos que se habían realizado frente a la profesionalización y el incremento de la Fuerza Pública (Rosanía et al., 2017).

De la seguridad nacional a la seguridad multidimensional

De acuerdo con el análisis historiográfico mostrado, en Colombia, la concepción de la seguridad era débil, pero había logrado avanzar, gracias a la consolidación de las fronteras, a la profesionalización del poder militar del Estado y al fortalecimiento del poder político. La funcionalidad de las FF. AA. en el país se basaba en el cumplimiento de labores policiales que impidiesen la desmembración nacional, bien por actores internos, o bien, por externos. Así, solo con la llegada de la Constitución de 1886, la profesionalización de 1909 y la guerra contra el Perú, en 1932, se ampliaría a la protección de la frontera. Sin embargo, si algo deja claro la historia del país es que las FF. AA. nunca han tenido que realizar actividades militares a gran escala contra un enemigo externo, excepto por el conflicto colombo-peruano de 1932, lo que se presentará de manera aún más evidente con el ingreso de nuevas ideologías a los contextos nacional e internacional.

Los primeros acercamientos de Colombia a la nueva realidad internacional posterior a la Segunda Guerra Mundial tuvieron que ver con un mayor acercamiento a Estados Unidos, lo que garantizó un impulso en la tecnificación y la actualización de la doctrina militar de las FF. AA. Aunque los principales acercamientos se dieron en 1942, con la presidencia de Eduardo Santos, fue para los primeros años de la década de 1950 cuando la relación se estrechó. A consecuencia de ello, en 1950 el país se embarcó en una expedición militar que cambiaría el modo de luchar de las FF. AA. y la caracterización de la seguridad

nacional. La guerra de Corea fue, para el pensamiento de la seguridad nacional en Colombia, un importante punto de integración con la doctrina militar estadounidense.

El conflicto en Corea significó para la conceptualización de la seguridad un importante cambio en la idea que se venía llevando durante los siglos XIX y XX, ya que Colombia se adhería a las nuevas tendencias en el campo de batalla, y ahora se posicionaba con firmeza en la misma esfera política del país del norte, que, a su vez, cumplía las labores de hegemonía hemisférica y global. En tal medida, los políticos colombianos lograron que la seguridad nacional formase parte del sistema internacional; es decir, que hiciera parte de las dinámicas propias de la Guerra Fría. Sin embargo, para lograr tal objetivo, los gobernantes debían entender que la Fuerza Pública no era un mero instrumento para garantizar el orden interno o tan solo para luchar contra las amenazas tradicionales, que se veían representadas en las guerrillas colombianas (Ugarriza & Pabón, 2018).

A la llegada de oficiales veteranos de la guerra en Asia, como Álvaro Valencia Tovar, Alberto Ruiz Novoa o Gabriel Puyana García, se intentó incluir estos nuevos conocimientos en la realidad militar de Colombia. Uno de los más interesados en esto fue el general Alberto Ruiz Novoa, quién escribió en 1956 el libro *Enseñanzas militares de la campaña de Corea*, esencial para el entendimiento de la introducción de todo lo aprendido y para su aplicación en el caso colombiano, si bien, según el mismo autor, resultaba imposible aplicar algunos puntos en la realidad nacional (Rodríguez, 2006).

Por su parte, el general Álvaro Valencia Tovar describió que la guerra revolucionaria, propuesta como un reductor de las asimetrías entre combatientes, se convertía en una grave amenaza al Estado nación y a su ciudadanía, de tal forma que, necesariamente, "el pueblo y el Ejército deben adquirir una conciencia ofensiva dentro del campo de la defensa nacional. Ofensiva en el sentido de aniquilar el morbo revolucionario antes de que se propague como infección incurable" (Valencia, 1964, p. 98). Lo anterior, por tanto, respondía a una nueva concepción de seguridad, basada en la unión de las capacidades del Estado en su totalidad, y no solo en materia militar, como había sido llevada a cabo hasta el momento (Valencia, 1964). Durante estos años, el pie de fuerza creció de manera exponencial, ya que en 1955 el gasto militar del país aumentó, a su vez, en el 55 % con respecto del año anterior, y se acercó al 20 % del presupuesto anual (Rosanía et al., 2017).

Entre los elementos de mayor importancia de los avances realizados en la lucha contrainsurgente se encuentran dos: en primer lugar, la implementación del Plan Lazo, por parte del general Alberto Ruiz Novoa, en 1964, y que buscaba

> […] emprender y realizar la acción civil y las relaciones militares que sean necesarias para eliminar las cuadrillas de bandoleros o prevenir la formación de nuevos focos o núcleos de antisociales a fin de obtener y mantener un estado de paz y tranquilidad en todo el territorio nacional. (Ugarriza & Pabón, 2018, p. 71)

Fue a partir de ese hito cuando se establecieron los primeros elementos de la acción integral y la acción conjunta, que en la actualidad hacen presencia en todo el aparato militar colombiano.

A fin de evitar el posible ingreso del comunismo en las sociedades del continente, Estados Unidos instauró el principio de seguridad denominado Doctrina de Seguridad Nacional, basada en la protección de los elementos esenciales de las naciones americanas en contra de un enemigo que buscaba la afectación de dichos elementos, como ente social (Leal, 2003); con ello, según Leal (2003), la Doctrina de Seguridad Nacional afectaría tanto a países con presencia de cuerpos castrenses en las más altas esferas del poder político como aquellos donde el poder militar se mantuvo subordinado al poder civil; entre estos, Colombia. Con ello se planteó que la lucha ideológica que vivían los países era causada, principalmente, por la pugna ideológica traída por el comunismo; por ende, para poder desarrollarse, era necesario derrotarlo. Aquello, por tanto, logra enmarcar el conflicto armado colombiano en una dinámica internacional importante.

En el caso de Colombia, las FF. AA., como ya se dijo, nunca buscaron subyugar el poder civil al propio; no obstante, la implementación del nuevo Estatuto de Seguridad, del presidente Julio César Turbay Ayala, permitió acciones a las actividades militares que buscaban la defensa de la sociedad permeando la doctrina estadounidense en sus acciones (Vargas, 2008). De ese modo, en el país se dio un fuerte enfrentamiento entre las acciones guerrilleras y unas FF. MM. cada vez más acostumbradas a la lucha contrainsurgente, tanto por aprendizajes propios como por los insumos entregados por Estados Unidos en la dinámica bipolar. De acuerdo con Vargas (2008),

> El gobierno Turbay Ayala (1978-1982) inauguró su mandato con la promulgación del Decreto legislativo 1923 de 1978, conocido como Estatuto de Seguridad. Con ese decreto y el respaldo pleno del presidente, las instituciones militares ampliaron su autonomía en el manejo de los asuntos de orden público a

> niveles sin precedentes, en lo que fue el ejercicio más completo de asimilación colombiana de la Doctrina de Seguridad Nacional suramericana. (p. 330)

Con la entrada en escena del narcotráfico, durante las décadas de 1980 y 1990, la guerra de guerrillas se incrementó. La seguridad nacional pasó a ser convertida en la lucha contra los grupos armados que pretendían poner de rodillas la institucionalidad del país; así, el ingreso de nuevos actores criminales difuminó la capacidad de las FF. AA., y fueron los años noventa del siglo XX el peor momento para las fuerzas del orden. Acciones como las vistas en Miraflores, el cerro de Patascoy, el cerro Tokio y Las Delicias, entre muchos otros golpes, demostraron que ni la concepción ni la estrategia de seguridad en Colombia estaban correctamente encaminadas, y no lograban rechazar las amenazas criminales, que ahora eran impulsadas por el narcotráfico (Ugarriza & Pabón, 2018).

De acuerdo con el general Mora Rangel (Nova, 2019), la dinámica del narcotráfico, aunque pequeña, nació desde el decenio de 1940, con la marihuana; sin embargo, fueron las guerrillas —primero, mediante el impuesto a los cultivadores, y luego, con el control total del proceso productivo— las que lograron repotenciar una lucha armada que se veía, para finales de la década de 1980, como desgastada y sin futuro. Por tal motivo, las guerrillas lograron controlar todo el fenómeno del narcotráfico, y convertirse así en un cartel más.

En las FF. AA. se inició un proceso de reestructuración, donde el tradicional concepto de un ejército pequeño había quedado atrás desde los años ochenta del siglo XX, al pasar de 59.568 efectivos en 1974 a 160.000 en 2002 (Centro de Estudios Históricos del Ejército, 2007). En 2015 el Ejército se componía de 220.537 efectivos, de los 265.050 de la totalidad de las FF. MM. (Resdal, 2016), y se llevó a cabo la creación de unidades de despliegue rápido y de unidades de aviación del Ejército, más el reforzamiento de las capacidades anfibias y el fortalecimiento de unidades de acción integral, entre muchos otros. De acuerdo con Mora Rangel (Nova, 2019), el Plan Colombia, gran accionador de la modernización de las FF. AA. en el país, fue una feliz coincidencia con la restructuración del Ejército Nacional, que buscaba luchar contra el narcotráfico, pero que, con la llegada del impulso antiterrorista de Estados Unidos de 2001, tras los ataques contra el World Trade Center, se transformó en un esfuerzo por combatir el terrorismo en el territorio nacional. A continuación, se daría el impulso del gobierno de Álvaro Uribe Vélez, con la Política de Defensa y Seguridad Democrática, que debilitó la capacidad militar de las FARC y logró la desmovilización de las Autodefensas Unidas de Colombia (AUC) (Cimadevilla, 2019).

La ofensiva militar de las FF. AA. contra la criminalidad, mantenida durante el gobierno del presidente Juan Manuel Santos Calderón, si bien cambió con la implementación en los cuerpos castrenses de un nuevo modelo de seguridad, alejado de la concepción de seguridad nacional contrainsurgente, el cual se enfocaba solo en la defensa de la integralidad del territorio y en el reconocimiento de una única amenaza criminal armada irregular. En la Política Integral de Seguridad y Defensa para la Prosperidad (Ministerio de Defensa Nacional, 2011) de aquel gobierno, se enfatizaba:

> Las FF. MM. seguirán comprometidas en la salvaguarda de los intereses políticos, económicos y sociales de la nación y continuará el proceso de fortalecimiento de sus capacidades. Sin embargo, dada la naturaleza multidimensional de la seguridad internacional, se avanzará en el diseño e implementación de un sistema disuasivo de defensa creíble, integrado, y operable también para cumplir con los propósitos de seguridad interna. (p. 36)

En consecuencia, la inserción de las políticas públicas de defensa permitió que la seguridad multidimensional, conceptualizada en la declaración de Bridgetown de 2002, empezara a ser aplicada. En este enfoque de seguridad multidimensional, impulsado, principalmente, por los hechos del 11 de septiembre de 2001 y por el aumento de la observancia de Estados Unidos sobre las acciones terroristas, hace claridad respecto a la existencia de nuevas amenazas que van más allá de la tradicional concepción de la seguridad nacional basada en el Estado (Font & Ortega, 2012), tal como se había venido llevando a cabo en Latinoamérica; en especial, durante la época de la Doctrina de la Seguridad Nacional.

Por lo anterior, Colombia se ha integrado a un proceso que acepta la presencia de nuevas posibilidades de afectación, ya no al Estado como tal, sino a los ciudadanos, en una concepción personalista basada en la protección de la persona humana. Lo anterior, ligado a la idea de la seguridad humana del Informe de Desarrollo Humano de 1994, del Programa de las Naciones Unidas para el Desarrollo, en el que cambia el objetivo del enfoque de la seguridad (Carvajal, 2008).

En el caso colombiano, la seguridad multidimensional tiene un reflejo aún más importante en las políticas públicas de seguridad. En primer lugar, la transformación de las amenazas, tal como lo expone Cimadevilla (2019), liga el direccionamiento de la guerra hacia la concepción de las nuevas guerras, y expone una ampliación del concepto de seguridad y de la función de las FF. AA. De igual

manera, en segundo lugar muestra un aumento en el portafolio criminal de los grupos armados y una mutación en su formulación. Es decir, con el fin de lograr sus intereses, los grupos criminales se han transformado en grupos de redes, y no en elementos jerarquizados; por tanto, la construcción de la estrategia de la seguridad ya no responde a un típico conflicto armado, en el que se quiere acabar con las cabezas principales de los grupos armados, sino en la necesidad de desmantelar las principales fuentes de financiación y desincentivar el nacimiento de nuevos grupos que ocupen aquel lugar. Lo anterior es categóricamente más complicado en un mundo criminal ampliamente globalizado; sobre todo, en el caso colombiano, en el cual los carteles mexicanos tienen grandes intereses sobre la producción de narcóticos. La Política Pública de Defensa y Seguridad (Ministerio de Defensa Nacional, 2019), del presidente Iván Duque Márquez, expone al respecto:

> Esta Política responde a las amenazas y a los desafíos de seguridad, desde un nuevo enfoque multidimensional y con el fin de fortalecer la legitimidad estatal y el régimen democrático, el respeto por los derechos humanos y la construcción de legalidad. (p. 5)

Al mismo tiempo, indica:

> Hoy, se requiere una nueva visión de seguridad que amplíe el objetivo de confrontar a esos grupos armados y las economías ilícitas y de paso a adoptar una política de carácter multidimensional que atienda los intereses nacionales, consolide el Estado de derecho, fortalezca la legitimidad democrática de las instituciones, garantice el respeto de los derechos humanos y se convierta en el motor de la transformación estructural de los territorios afectados por la criminalidad y la violencia, asegurando su incorporación plena al conjunto de la nación y denegándoselos a los grupos ilegales. (p. 20)

En consecuencia, la formulación de la propuesta de la seguridad cambia sustancialmente: ahora se abren espacios más amplios de interrelación del poder militar con respecto a las actividades del Estado, al asignársele unas nuevas actividades de gran importancia; además, se potencia la Consejería Presidencial de Seguridad Nacional y se activa el Consejo de Seguridad Nacional como órgano asesor, tal como lo enuncia la Política:

> En ese orden, la legalidad, el emprendimiento y la equidad, pilares del Gobierno nacional tienen como base la defensa y la seguridad, concebidas más allá del despliegue operacional de Fuerzas Militares y de Policía Nacional, es decir, una defensa y seguridad que implica la acción unificada del conjunto de las

> instituciones del Estado. Denegar los espacios a las organizaciones armadas ilegales solo puede ser posible con una transformación de la forma en que el Estado busca la desarticulación de dichas organizaciones en los territorios y en la que estos son abordados por el Gobierno y la justicia (p. 20)

En conclusión, a lo largo del análisis historiográfico mencionado se encuentran varios elementos que han logrado moldear la concepción de seguridad y su evolución en Colombia. En primer lugar, la dificultad geográfica de la nación no permitió durante el siglo XIX la consolidación de un sentimiento nacional arraigado a un territorio, sino que, más bien, impuso a un Estado que carecía de nación, lo cual, gracias a esfuerzos de diversas clases: esfuerzos políticos, como las constituciones y las políticas de seguridad; simbólicos, como el himno o los elementos representativos de la nación colombiana, y militares, como constructores del ejercicio del uso de la fuerza indisputable del Estado. En segundo lugar, la conflictividad interna inmersa en las dinámicas históricas de cada momento, desde el desarrollo del proceso imperialista del siglo XIX hasta la inmersión de la bipolaridad ideológica de la segunda mitad del siglo XX, y su impacto en la seguridad nacional, entre varios otros. Con ello, resulta claro que Colombia ha tenido un complicado paso de la seguridad nacional clásica de tipo realista a la multidimensionalidad; sin embargo, se ha logrado entrar poco a poco en las nuevas dimensiones de la seguridad mundial. Todo esto llevaría a ver un cambio importante en el desarrollo de las actividades de las FF. MM. del país, como se verá a continuación.

Rol de las Fuerzas Militares en Colombia

Las FF. AA. ahora tienen una funcionalidad distinta, de acuerdo con la época y las circunstancias en las que se han enmarcado. Según Nicolás Maquiavelo (1520/2011), resulta necesario que un Estado consolide su propia fuerza armada, y se aleje así de los tradicionales mercenarios, o soldados pagados. Con ello en mente, el Estado nación ha comprendido que la base de su ejercicio del poder se centra en el monopolio de la fuerza. Será en dicha función donde las FF. MM., como únicos valedores de la fuerza física del Estado, puedan ejercer la soberanía en el territorio regulado entre los países vecinos, y este, llegado el caso, hacer uso de la violencia (Rosanía et al., 2017).

La funcionalidad de las FF. MM. se ha mantenido en dos campos importantes. El primero es la materialización de los intereses políticos de las naciones en el campo de batalla, al otorgarse la capacidad de estos para construir los

planes de guerra que se realizan en una confrontación internacional, o guerras defensivas por el territorio soberano (Calvo, 2013). Así, en segundo lugar, está el uso del monopolio de la fuerza para mantener el control del orden interno, que, en gran medida, se les ha otorgado a los cuerpos de gendarmería o de policía, dependiendo de la época.

Con todo, la evolución de las actividades de la Fuerza Pública ha crecido forzosamente, y no solo en Colombia, donde el contexto militar ha variado a la normalidad internacional a causa de los motivos ya mencionados. Así, con el paso del enfoque de seguridad clásico, surgido del siglo XIX y de los procesos históricos en el siglo XX —entre ellos, la Segunda Guerra Mundial y la Guerra Fría—, a la seguridad multidimensional, las actividades han cambiado; sobre todo, en momentos de graves crisis, como la que ahora mismo enfrenta el planeta por la pandemia del Covid-19.

Con el fin de la Segunda Guerra Mundial, la guerra cambió para siempre y de forma radical. La concepción westfaliana del Estado se ha debilitado, al adquirir protagonismo otros actores que antes habían administrado el monopolio de la fuerza. De acuerdo con Lind y Thiele (2015), tras la Segunda Guerra Mundial han surgido actores y causas de conflicto que antes de 1648 existían, pero hoy coexisten con Estados nación, modernos y consolidados. De esta manera, movimientos étnicos, religiosos, políticos, e incluso económicos, han usurpado el uso de la violencia en los Estados impulsando conflictos causados por dichos intereses, que mantienen en constante furor luchas armadas de baja intensidad, pero de enormes implicaciones humanitarias. Con ello, los métodos de conflicto irregular han ido presentándose como la normalidad en el desarrollo de actividades bélicas internacionales y no internacionales.

Esto se evidenció, principalmente, en la guerra de Vietnam. Estados Unidos ha mostrado su interés en comprender dichos tipos de conflictos armados irregulares, híbridos y asimétricos; por tal motivo, han formulado una variación en las actividades militares que se alejaron sustancialmente del rígido actuar de la guerra de primera, de segunda y de tercera generación, descritas por Lind y Thiele (2015).

En Colombia se ha logrado establecer elementos en las ramas de la Fuerza Pública dedicada a ese tipo de operaciones. Con el nacimiento de la guerra irregular en el país —en especial, por las guerrillas comunistas durante los años sesenta del siglo XX—, se establecieron actividades inusuales para los cuerpos armados; entre ellas, el uso de la acción integral. Esta actividad, ligada a

las operaciones militares distintas de la guerra, ha tomado gran relevancia en la Fuerza Pública colombiana; la reproducción de los planes de guerra, mencionados en el capítulo anterior, por el general Ruiz Novoa, como el Plan Lazo, el Plan Perla y el Plan Andes. Un claro ejemplo de estas nuevas actividades son las emisoras radiales de las FF. AA.; durante las presidencias de Uribe Vélez y Santos Calderón, el aumento de estaciones radiales de la Armada Nacional (ARC) y del Ejército Nacional (EJC) creció de forma sustancial, y logró un importante impacto en la moral de las propias tropas, mediante la utilización de la música y de los mensajes de apoyo a los hombres emplazados en los más alejados rincones del país, y en contra de las fuerzas subversivas, que sufrieron un amplio número de desmovilizaciones (Bock, 2019).

Por otra parte, el desarrollo de nuevos enfoques de seguridad también ha otorgado a la Fuerza Pública funciones que otrora no se consideraban propias de ella. Cabe recordar que el concepto de seguridad nacional, usado de manera tradicional durante los siglos XIX y XX, concretaba la funcionalidad y los roles de las FF. AA. en la seguridad, en el uso del monopolio de la fuerza y en el accionar del poder militar de los Estados para satisfacer sus intereses nacionales; sin embargo, con el fin de la Guerra Fría, la creación de los nuevos enfoques humanistas —incluyendo la seguridad humana y la seguridad multidimensional—, ha otorgado a las FF. AA. funciones que las han acercado, ciertamente, a la población civil. Las acciones integrales han disminuido su funcionalidad como solo destinadas a operaciones distintas de la guerra, y por eso han logrado apoyar a la población civil en caso de graves afectaciones humanitarias (Castillo, 2019), como en la actualidad, la pandemia del Covid-19. La Operación San Roque, aunque esté enmarcada en un esfuerzo de las FF. MM., ha logrado buscar, en una acción coordinada de las FF. AA., la ayuda a la ciudadanía con elementos de primera necesidad. El presidente Duque Márquez la llamó la "operación humanitaria más grande en la historia de Colombia" (*BC Noticias*, 2021, párr. 2).

Aquello no ha sido lo único: la Fuerza Pública también ha encontrado que las economías ilegales utilizadas por grupos armados han afectado gravemente la capacidad hídrica y natural del territorio nacional; sobre todo, los grandes bosques selváticos, que abundan a lo largo del territorio nacional. De esta manera, se ha buscado el mantenimiento de espacios ambientales estableciendo operaciones que mitiguen las afectaciones; entre ellas, la Operación Atalanta, creada durante el gobierno del presidente Santos Calderón, y mantenida durante el gobierno actual.

Para terminar, resulta claro que la evolución al concebir la seguridad ha cambiado los roles de las FF. MM.; todo esto, debido al claro aumento en las amenazas que se perciben con los nuevos enfoques; con ello, resulta evidente que en un país como Colombia, donde la Fuerza Pública es una de las pocas entidades que logran abarcar la totalidad del espacio geográfico, deberán ampliar su rango de acción, y permitir que las nuevas disposiciones en las políticas públicas de seguridad —dentro de las que se incluye la multidimensionalidad de la seguridad— les otorguen actividades que antaño no resultaban claras. A continuación, se hará un análisis más detenido a esta evolución, desde la perspectiva de la FAC, encargada del ejercicio del poder aéreo en Colombia, y el cambio que ha significado en sus actividades el nuevo entendimiento de la seguridad.

Recuento histórico del rol de la Fuerza Aérea Colombiana durante los tiempos de la seguridad nacional y la seguridad multidimensional

La Evolución del Poder Aéreo

A comienzos de 1900, en la pequeña ciudad de Kitty Hawk, ubicada en el estado de Carolina del Norte, Estados Unidos, durante varios años los hermanos Orville y Wilbur Wright intentaban llevar a cabo un vuelo en una máquina con motor; varios intentos fallidos y su perseverancia hicieron que el sueño de volar se cumpliera el 3 de diciembre de 1902. A partir de ese hito, la aviación se convirtió en una búsqueda constante, por parte de las grandes potencias, en pro mejorar los resultados y hacer del nuevo invento un elemento útil para la ciudadanía, y para su uso militar. Con el tiempo, Estados Unidos, Francia, Rusia, Alemania, Italia e Inglaterra comenzaron a visualizar las capacidades de los artefactos en su aplicación militar, e iniciaron la estructuración de lo que hoy se conoce como *poder aéreo* (Macisaac, 1992). Tal carrera llevó a que se establecieran los primeros modelos teóricos y prácticos para el uso de los nuevos aparatos, en la búsqueda de satisfacer los intereses nacionales de cada país.

A pesar de eventos como la guerra Ítalo-turca, en 1911, fue, en realidad, la Primera Guerra Mundial (1914-1918) la que dio el pistoletazo inicial para la ejecución de los planes militares aéreos a favor de las estrategias nacionales (Barrero-Barrero & Olarte, 2020). En agosto de 1914, el mundo vio con horror

el comienzo de la Primera Guerra Mundial, como resultado del asesinato, en Sarajevo, del archiduque Francisco Fernando, heredero del trono austrohúngaro. Para esa época, el avión era utilizado como un factor experimental, pero con el tiempo terminó siendo decisivo, por el miedo que infundía a las tropas en tierra, al ser las aeronaves el anuncio de enormes andanadas de artillería sobre sus posiciones. De esta manera, su primera función como elemento militar se consolidó en el reconocimiento aéreo visual y probar la puntería de las piezas artilleras (Montgomery, 1969).

Se puede concluir que una primera misión de la aviación militar para esa época era disuadir, afectar psicológicamente al enemigo y llevar a cabo misiones de reconocimiento visual, más allá de la ubicación de las propias tropas. Esto derivaba, por tanto, en una competencia teórica, metodológica y armamentista entre las potencias mundiales para obtener mejores aeronaves de combate que abarcaran todas las especialidades, lo que, a su vez, llevó al nacimiento, entre otros, del avión caza y del bombardero, que rivalizaban, de esa forma, con otros artefactos aeronáuticos como el dirigible de helio, más comúnmente llamado Zepelín (Macisaac, 1992).

Fue después de la Primera Guerra Mundial cuando teóricos militares como Gulio Douhet —creador de los conceptos *dominio* o *superioridad* aéreos— añadieron a las concepciones de la guerra las de los tomadores de decisiones militares, y cuando se volvió importante el control del aire, en un proceso de tecnificación aérea constante (Meza, 2016). De acuerdo con Van Creveld (2015), Douhet consideraba que, cuando se lograra sobrepasar obstáculos terrestres y marítimos, el poder aéreo se convertiría en el ejercicio decisivo de la guerra, al ser capaz de destruir cualquier resistencia armada y cualquier moral con el uso de reducidos esfuerzos económicos y militares, y se hizo objetivo del poder aéreo el ataque a las zonas de importancia económica del enemigo para el sostenimiento de las acciones bélicas.

En la Segunda Guerra Mundial, las teorías de Douhett, junto con las de otros teóricos del poder aéreo, como Mitchell y Seversky, impulsaron la utilización de los aviones como elemento clave del empuje militar en el campo de batalla (Macisaac, 1992). Así, el avión de combate, mucho más desarrollado, se convirtió en una potencia destructora, y apareció aquí otro concepto de los principios de la guerra denominado *alcance*.

El avance tecnológico dio paso a la conceptualización de elementos como el *alcance*; o sea, la capacidad para extender la acción bélica y los ataques justo

al corazón del enemigo. Las fuerzas aéreas empezaron a desarrollar con más flexibilidad actividades militares y de combate; esto es, a realizar diferentes misiones de acuerdo con las necesidades operacionales. La velocidad y la versatilidad dan la capacidad para penetrar y llegar a objetivos militares vitales para la supervivencia del enemigo, bases militares, centros de comando, refinerías, vías, comunicaciones y centros urbanos, entre otros (Sotelo, 2016).

Con la Guerra Fría, los esfuerzos por mantener un elemento de poder aéreo fuerte se han mantenido como uno de los principales objetivos de las grandes potencias. En la actualidad, Estados Unidos, China, Rusia, Gran Bretaña y Francia buscan en la tecnología la protección de sus propios espacios aéreos de posibles acciones bélicas contra sus intereses nacionales. Ello resulta en especial relevante cuando se habla de *beligerancia nuclear*, y en momentos en que son los misiles y los bombarderos con capacidad nuclear elementos clave para reproducir las estrategias de disuasión limitada o del uso ofensivo de estas (Macisaac, 1992).

La Fuerza Aérea Colombiana, de la Seguridad Nacional a la Seguridad Multidimensional

Durante la época en que se estructuraba el concepto de poder aéreo en los cielos de Europa, en América —especialmente, en la República de Colombia— se daban los primeros pasos para instalar una verdadera Fuerza Aérea. A pesar de la distancia, muchos países seguían de cerca la situación del conflicto en Europa y se conocían los terribles daños materiales y las pérdidas humanas, lo cual motivó a un grupo de personas a presentar proyectos para el desarrollo y el inicio de la aviación militar en Colombia. El 7 de septiembre de 1916 se expidió la Ley 15, que dio vida a la especialización aeronáutica del Ejército (Villalobos, 1993). La mencionada ley facultaba al Gobierno para enviar, en comisión de estudios al exterior, a oficiales de diferentes armas y especialidades, a fin de recibir instrucción y entrenamiento de vuelo, mantenimiento, técnicas y tácticas para el combate.

El artículo 8 de dicha ley obligaba al Gobierno nacional a crear una Escuela de Aviación Militar que contara con maestros y directores a cargo del correcto entrenamiento de los nuevos pilotos (Villalobos, 1993). El uso de la aviación de combate en las distintas guerras mostró la necesidad de que la organización militar creara definitivamente unidades aéreas. El 31 de diciembre de 1919, mediante la Ley 126, el presidente Marco Fidel Suárez estableció la aviación como arma del Ejército y autorizó al Gobierno para llevar a cabo la reglamentación, las disposiciones y las órdenes para proveer la dotación de personal y material

de esta nueva arma, a la cual se consideró, un año después, la quinta arma del EJC, lo que obligaba a aquellos soñadores del aire a entrenarse en la Escuela de Aviación Militar para obtener sus alas (Useche, 2019).

La Escuela de Aviación Militar fue fundada dos años después, y se la ubicó en el municipio de Flandes, en el departamento de Tolima, y allí se entrenaron los primeros pilotos de Colombia en aviones tipo Caudron G3 y G4, de procedencia francesa (Hernández, 2020). El Gobierno nacional adquirió los primeros aviones en Francia, y una comisión de pilotos y técnicos llegaron al país para dar instrucción y entrenamiento a los oficiales y los suboficiales asignados a la aviación en la recién creada Escuela de Aviación Militar (Useche, 2019). También, en los años siguientes, llegaron a Colombia misiones desde Alemania, Estados Unidos y otros países, que apoyaron de manera importante el desarrollo de la aviación militar nacional.

Sin embargo, la escuela fue clausurada desde 1922 hasta 1925, y fue trasladada al municipio de Madrid, Cundinamarca. Así fue la tendencia de la escuela, entre cierres temporales y cambios de misiones, hasta 1929 (Villalobos, 1993). Cabe anotar que la escuela tenía un elemento dicotómico entre la aviación civil y la aviación militar, y fueron entrenados pilotos para ambos tipos de aviación, con lo cual se reparó en la necesidad de mantener pilotos colombianos en la nueva disciplina. Pero eso cambió cuando el 1 de septiembre de 1932 el Ejército del Perú invadió Leticia.

Así, en un "corto lapso de 90 días se organizó una fuerza militar con escuadrones de la Fuerza Aérea Colombiana (FAC), tripulados por aviadores colombo-alemanes, pilotos de la Sociedad Colombo-Alemana de Transportes Aéreos (SCADTA), incluyendo la legendaria figura del coronel Herbert Boy" (Pérez, 2016, p. 28). En ese momento se hizo el primer bombardeo aéreo en un conflicto americano: fue en el puerto de Tarapacá, por parte de un grupo de aeronaves colombianas. Gracias a esto, las capacidades aéreas de Colombia aumentaron de manera importante. Según Parra (1998), el presidente Olaya Herrera "quiso comprar infructuosamente al gobierno de los EE. UU. dos aviones anfibios. Colombia logró adquirir a fabricantes privados norteamericanos y europeos una verdadera flotilla, que adicionada con aparatos adquiridos internamente sumaba 36 aviones" (p. 110), que se dividirían en cuatro bombarderos pesados (tres Consolidated y un Dornier Wal), un bombardero liviano (Junkers), dos aviones pesados de observación (Dornier Bluebird), 25 aviones de combate (trece Curtis Hawk, diez Curtis Falcon y dos Curtis Osprey), siete aviones de transporte (cinco

Junkers, un Hamilton y un Dornier Wal) y catorce aviones de entrenamiento (seis Curtis Fledgling y ocho Curtis Trainer) y, por último, seis aviones de despacho (Wild) (Parra, 1998).

Por esto mismo, la historia reconoce la acción valerosa de la aviación militar para la recuperación del territorio, no sin antes encomiar los ingentes esfuerzos del Gobierno y la ciudadanía en pro de contribuir a la modernización de los equipos, factor fundamental para la victoria. Se puede en este punto deducir que el Gobierno y los altos mandos militares entendieron la importancia del poder aéreo, su empleo, su alcance, su movilidad, su factor sorpresa y otros principios básicos de la guerra utilizados durante el conflicto.

Una vez terminado el conflicto con el Perú, hubo muchas recomendaciones y elogios a la participación y las acciones militares de la aviación, y se cumplieron misiones prioritarias de observación, bombardeo e inteligencia, y a fin de explotar la capacidad para mover rápidamente personal y equipo a las zonas de combate. Se inició así el proceso de crear una organización autónoma, dependiente del Ministerio de Guerra y del Comando de las FF. MM., y con una misión y una organización autónomas. El 15 de julio de 1942, el Gobierno nacional expidió el Decreto 1680, por medio del cual el arma táctica de la aviación militar pasó a ser una institución independiente, y así las FF. MM. quedaron conformadas por el EJC, la ARC y la Fuerza Aérea Nacional, como se la denominó en su momento (Domínguez, 2018). Obviamente, se requería el apoyo de oficiales del Ejército para formar los cuadros y el escalafón de la nueva institución, con lo que se logró graduar cada año un buen número de pilotos y oficiales de otras especialidades, necesarias para el desarrollo de las misiones por cumplir.

Con el tiempo, la FAC se vio inmersa en el conflicto armado que tenía lugar en el país, pero tampoco fue ajena a los avances en la concepción de seguridad que se dieron en las otras dos fuerzas del poder militar colombiano. De acuerdo con Esquivel (2015),

> La escasa historiografía sobre la Fuerza Aérea en el conflicto colombiano solo describe el cambio desde un ocasional suministro de apoyo aerotáctico al Ejército Nacional, en operaciones de contraguerrilla (Villalobos, 1993, pp. 246, 336), hasta el permanente alistamiento para operaciones conjuntas y de combate directo. (pp. 380-381)

A raíz de la naturaleza del devenir político del Estado, y por el trascurso de la violencia del país —especialmente, con posterioridad a los años cincuenta del siglo XX, cuando la guerra irregular se presentaba en amplios espacios del territorio

nacional—, hubo una importante reducción en las capacidades de la FAC. De acuerdo con Conde (2016), "se disminuyó el flujo de recursos para el estamento militar y por consiguiente soportar las operaciones aéreas afectando de manera directa el desarrollo y evolución del poder aéreo" (p. 157). Sin embargo, gracias al empuje de oficiales como el general Alberto Pauwels Rodríguez, se logró activar en 1956, por primera vez en la historia del país, un proyecto de industria aeronáutica, con el nombre de Corporación de la Industria Aeronáutica Colombiana (CIAC), con el fin de proveer un mantenimiento nacional de las aeronaves civiles y militares, así como la construcción del actual Aeropuerto Internacional El Dorado, de Bogotá (Conde, 2016).

Asimismo, en esos años hubo un aumento importante en las capacidades de la FAC, cuando ingresó al país un cierto número de helicópteros que tuvieron como destino la Base Aérea de Melgar; además, se integraron aeronaves a propulsión de entrenamiento RT-33A Shooting Star, para posteriormente ingresar los poderosos F-86 Mark IV y F-86F; ambos, de tipo Sabre (Soler, 1988). Y por último, en 1962 se fundó el Servicio de Aeronavegación a los Territorios Nacionales (Satena), el cual fue entregado a la FAC para su administración (Conde, 2016).

Aquella labor de la FAC, en consonancia con la evolución del desarrollo de los conceptos de seguridad nacional que se iban gestando en medio del conflicto armado colombiano, hizo que para comienzos de los años setenta y finales de los sesenta del siglo XX se evolucionara a una Fuerza Aérea enfocada en la contención del orden público, de tal manera que las aeronaves se convirtieron en plataformas para la lucha contraguerrillera.

De acuerdo con De la Cruz (1978), en su función contraguerrillera la FAC se mantuvo en su función de crear una plataforma aérea para el apoyo de las actividades en tierra. Así, aviones como el C-47, el C-130 o el 46-A Beaver apoyaron como plataformas de despliegue rápido de tropas del Ejército en lugares de urgente necesidad, a causa de las actividades guerrilleras. Aunado a lo anterior, estos aviones funcionaron como eficientes puntos de interdicción aérea y ataque en contra de zonas estratégicas del enemigo, como campamentos y centros de abastecimiento y de apertrechamiento, entre otras.

Para seguir con esta creciente tendencia al aumento de las capacidades helicoportadas de la FAC, se logró aumentar la presencia de la Fuerza en el conflicto. Esto permitió que se llevaran a cabo actividades de reconocimiento, adiestramiento, evacuación médica, observación del campo de batalla y transporte rápido de tropas. Helicópteros como los OH13 H Siuox, los UH-1 Iroquois

o los UH-19 Chikasaw, se presentaron en batalla y permitieron una reducción de la niebla de guerra que presentaban las tropas del Ejército en tierra, el transporte de pertrechos y víveres para las tropas propias, de manera mucho más eficiente y segura que las realizadas por los aviones, entre otros, lo cual produjo una poderosa sinergia que empoderó al EJC en contra de las guerrillas (De la Cruz, 1978).

Ahora bien, en cuanto a su función de cuidar los aires de Colombia, durante el gobierno del presidente Misael Pastrana Borrero se inició la reforma tecnológica de la Fuerza a través de la compra de capacidades tecnológicas como el Mirage M-5 francés, posteriormente reemplazado por el avión de combate Kfir, de procedencia israelí, en 1978, y ambos, con la intención de realizar operaciones de interdicción aérea. Luego se agregaron aviones de combate como el Dragon Fly A-37B, en 1978, y el Tucano T-27, en 1992 (Hernández, 2017).

En los años ochenta y noventa del siglo XX, la FAC mantuvo sus actividades para sostener la soberanía del espacio aéreo, la integridad territorial y la lucha antiguerrillera; sin embargo, también empezaron a agregarse al repertorio operaciones de ayuda humanitaria, como: el "terremoto en Popayán (Cauca, marzo de 1983); desastre en Armero (Tolima, noviembre de 1985); desastre del río Páez (Cauca, junio de 1994); terremoto en el Eje Cafetero (enero de 1999)" (Esquivel, 2019), así como acciones contra el narcotráfico y sus delitos conexos.

Con esto en mente, se empezó a pensar en una FAC con mayor capacidad móvil para luchar contra las nuevas amenazas; especialmente, el narcotráfico y el contrabando. En cuanto a lo primero, fueron comunes las operaciones de interdicción de avionetas cargadas por los carteles de la droga, y se dio, en un momento de extremada presión, la facultad a "la Fuerza Aérea para interceptar y derribar tales aeronaves previa autorización expresa del comandante de la FAC e informando a la Fiscalía. Para ello se usarían los aviones Kfir y Mirage, los radares del Centro Militar de Defensa" (Esquivel, 2019, p. 133). De esta manera, durante la década de 1990, la FAC se constituyó en un enemigo temible; sobre todo, en operaciones de gran magnitud, como Vuelo de Ángel, en 1998, contra las FARC.

Ya para el periodo 1998-2001, momento en el que gobernaba el presidente Andrés Pastrana Arango, se hizo una importante modernización de las FF. AA. Las lecciones aprendidas durante todo el conflicto, el apoyo de Estados Unidos y la extrema presión que se sentía en las grandes urbes nacionales por el asedio de los grupos guerrilleros y paramilitares, fueron suficientes para el nacimiento de una voluntad política y social en apoyo de los cuerpos castrenses. En este

sentido, el ya mencionado Plan Colombia transformó las capacidades militares e implantó un nuevo modelo de seguridad. El narcotráfico y el terrorismo se convirtieron en los primeros enemigos, y el concepto de lucha contraguerrillera se difuminaba en una lucha contra la delincuencia y el miedo.

Así, la implementación de planes de guerra como el Plan Patriota, elevó el número de efectivos del EJC, y obligó, de esta manera, a la FAC a tener mayor presencia en su rápida movilización, así como el bombardeo táctico contra cabecillas del secretariado de las FARC (Esquivel, 2015). El gobierno Uribe y la correcta implementación de las nuevas capacidades militares, procuraron que la FAC se convirtiera en la vanguardia de la ofensiva militar, al ser esta la principal amenaza a los grupos terroristas que se paseaban por las selvas del territorio nacional. Todo esto resultó en golpes como la Operación Delta, en 2002, y la Operación Odiseo, en 2011, entre muchas otras. Así, según Esquivel (2015), la FAC logró dos cosas claras: primero, reducir las operaciones de las FARC de 33 operaciones en 2003 a solo dos en 2010, y demostrar que existió un efecto disuasorio de las capacidades. Y, en segundo lugar, esta tendencia anterior permitió intensificar ataques estratégicos contra los cabecillas de la mencionada organización guerrillera.

Por otra parte, con el fin de dar una mayor claridad sobre la evolución de la FAC en sus aspectos más relevantes, la institución hizo un planeamiento de la estrategia a mediano plazo, que incluye la actualización de planes y documentos anteriores; o sea, el concepto operacional. Por lo tanto, y para hacer más clara la evolución de la FAC con respecto a la multidimensionalidad de la seguridad, la evolución y los cambios de acuerdo con la dinámica del conflicto, las políticas de gobierno y el pensamiento estratégico institucional en cada época.

En la misión 2003-2010, momento en el que se encontraba al mando de la Fuerza el general Héctor Fabio Velasco Chávez, se incluyó como misión principal de la FAC "ejercer y mantener el dominio del aire y conducir operaciones aéreas para contribuir a la defensa de la soberanía, la independencia, la integridad territorial nacional y el orden institucional" (Fuerza Aérea Colombiana [FAC], 2003), lo cual enfatiza la contribución a la defensa de la soberanía del país, a la independencia, a la integridad territorial y al orden constitucional, como sus misiones principales.

Aquello resultaba importante en un momento cuando no se tenía el control del espacio aéreo en su totalidad, por falta de equipos como radares, sistemas

de defensa aérea e integración de señales y comunicaciones, entre otros. Con el fin de mejorar sus capacidades para el cumplimiento de su misión, la FAC llevó a cabo procesos importantes de adquisición y renovación de equipos de vuelo, equipo de apoyo terrestre, armamento, entrenamiento de tripulaciones y técnicos en diferentes especialidades, en los cuales fueron de vital importancia los aviones de combate para la lucha contra el narcotráfico y la guerrilla.

Ante las amenazas del narcotráfico y de las guerrillas, la FAC ajustó su misión constitucional a través del Plan Estratégico Institucional 2006-2019, en el que el general Édgar Alfonso Lesmes Abad mantuvo la misionalidad de la Fuerza, pero fue más allá, y abrió una nueva dimensión al referirse al espacio aéreo, al desarrollo aeroespacial y a la necesidad de la Fuerza de ver más allá del espacio (FAC, 2006). De esa manera, buscó en la tecnología y la capacitación lograr estos objetivos, tanto para el uso civil y militar como para la vigilancia del medio ambiente, y para combatir la deforestación, los incendios, la minería ilegal y los cultivos ilícitos.

Para el periodo 2011-2030, el general Tito Saúl Pinilla Pinilla, comandante de la FAC, incluyó en la misionalidad nuevos elementos que son constantes en la seguridad multidimensional, como la lucha contra el crimen organizado transnacional (COT), el terrorismo, el narcotráfico, las crisis económicas y las crisis medioambientales. En esta nueva misionalidad, se interpretó la realidad del Estado colombiano y se contribuyó en la adaptación de las FF. AA. a las nuevas amenazas (FAC, 2011).

Para lograrlo, se buscó cumplir con la responsabilidad del dominio del espacio aéreo, ya fuese para la realización de las operaciones contra las amenazas tradicionales, o para aportar a la seguridad y el bienestar del pueblo colombiano. Por último, a consecuencia de la realidad internacional, se preparó a la FAC para cumplir con su máximo deber constitucional: la protección de la integralidad del territorio nacional, las fronteras y la población del país (FAC, 2011).

En 2017, durante el comando del general Carlos Eduardo Bueno Vargas, se llevó a cabo una transformación operacional y organizacional de la Fuerza, conocida a través del documento *Poder aéreo, poder transformador* (FAC, 2019b), y basada en una evolución constante, con un entorno cambiante y una coyuntura que vive el país (proceso de paz), lo cual requirió una transformación especialmente operacional para responder frente a las nuevas amenazas y a la mutación de las tradicionales. Hubo también un cambio enorme en la estructura organizacional, pero no una modificación de la misión existente.

Por último, durante el actual proceso, desarrollado por el general Ramsés Rueda Rueda, se elaboró el Plan Estratégico Institucional 2020-2042, en el que se realizó un proceso de prospección hacia la situación de la FAC para 2042. Un análisis que se hará en el próximo capítulo, como demostración de las capacidades de adaptación de la FAC a las nuevas amenazas.

Como se ha visto, la FAC ha cumplido una misión especial durante el conflicto armado en los siglos XX y XXI. La programación de esta Fuerza como consolidadora del poder aéreo en la seguridad nacional y en la actual seguridad multidimensional ha otorgado al aire una capacidad nunca antes vista, y ha tenido un carácter especial en Latinoamérica, donde, a causa de la fuerte presencia de fenómenos de criminalidad, las FF. AA. —y entre ellas, las Fuerzas Aéreas del continente— han logrado la implementación del poder aéreo a fin de mitigar las amenazas detectadas por la seguridad multidimensional (Barrero-Barrero et al., 2018). En Colombia, en un marco de posconflicto y un avance en la disminución de conflictos internacionales y no internacionales, las FF. AA., como se ha demostrado, han tenido que cambiar su funcionamiento para adaptarse a las nuevas amenazas no tradicionales y estructurales que afectan al Estado y a sus habitantes; de esa manera, la FAC ha ampliado sus actividades, siempre enfocadas en la seguridad. Así, de acuerdo con Barrero-Barrero et al. (2018)),

> Se puede deducir de lo anterior cómo el poder aéreo está inmerso en el compromiso para dar respuestas y soluciones a los problemas de la seguridad multidimensional; más aún, las teorías de los grandes pensadores del tema toman fuerza y permanecen aún más vigentes, puesto que refuerzan su papel fundamental en una doctrina propuesta por la OEA. Lo importante es hacer uso del poder aéreo en conjunción con la seguridad multidimensional, en un enfoque legítimo de los Estados, de primer orden y contundente en lo que se requiera. (pp. 75-76)

En conclusión, el camino de la FAC no se ha visto alejado de la transformación que ha sufrido el concepto de seguridad en Colombia. A pesar de que en ocasiones la FAC haya sido considerada un arma alejada del combate, por su posición aérea, no hay nada más ajeno a la realidad: desde sus inicios, la Fuerza ha estado inmersa en el desarrollo de las acciones bélicas en contra de las amenazas tradicionales, como la lucha contrainsurgente, y así ha entregado a las fuerzas de tierra, tal como lo había previsto Douhet, un apoyo insuperable para el éxito de sus misiones y el debilitamiento de los enemigos de la nación; sin embargo, la FAC no se ha detenido ahí. Con la llegada de los nuevos enfoques en

la seguridad, ha logrado involucrarse en una amplia variedad actividades; entre estas, la ciberseguridad, el apoyo para mitigar los efectos de los desastres naturales y sus efectos ambientales, y prestar ayuda a las actividades en contra de la pandemia del Covid-19, entre otras. A continuación, se analizará la forma como la FAC utiliza sus capacidades para enfrentar las nuevas amenazas, y su intención de aplicar, desde sus funciones, el concepto *seguridad multidimensional*.

Capacidad de la Fuerza Aérea Colombiana con respecto a las nuevas amenazas

La FAC, de conformidad con la Constitución Política de Colombia, "tiene como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional" (Constitución Política de Colombia, 1991, art. 217); a su vez, "propende por la preparación de sus integrantes para la efectiva conducción de la guerra y de operaciones militares en tiempo que no sea de guerra" (FAC, 2021).

Las operaciones y las acciones de la FAC se enmarcan en la Política Pública de Defensa y Seguridad "para la legalidad, el emprendimiento y la equidad", del presidente Duque Márquez, y la cual responde, desde una visión multidimensional de la seguridad, a los nuevos desafíos y las nuevas amenazas. Estas amenazas emergentes, según García (2016), "se refieren a los riesgos a que están sometidas las naciones del mundo después de la terminación de la Guerra Fría" (García, 2016, p. 1); y según la Junta Interamericana de Defensa (2021), "Están presentes en nuestras sociedades incluyendo terrorismo, delincuencia organizada, tráfico de drogas ilícitas, tráfico ilícito de armas, corrupción, los desastres naturales, deterioro del medioambiente, lavado de activos, así como todas las formas de ataques cibernéticos" (Junta Interamericana de Defensa, 2021).

Para dar respuesta a dichas amenazas emergentes y lograr los objetivos planteados en la Política Pública de Defensa y Seguridad, la FAC ha establecido un Plan de Desarrollo, que guía el *Plan Estratégico Institucional "Así se va a las estrellas". Estrategia para el desarrollo aéreo y espacial de la Fuerza Área Colombiana 2042*.

> Este plan se soporta en un análisis prospectivo que permite definir las principales características que debe tener la institución en los horizontes de tiempo 2022, 2030 y 2042, para responder eficazmente a las necesidades futuras de la nación en materia de defensa y seguridad. (FAC, 2020)

En la tabla 1 se señalan las características diferenciales de cada tiempo, con especial énfasis en la importancia de la transición del enfoque regional al enfoque global para 2042.

Tabla 1. *Características diferenciales de la Fuerza Aérea Colombiana en cada tiempo*

2022	2030	2042
• Innovadora, polivalente, interoperable en ejercicios multinacionales con alcance regional. • Referente regional. • Capacidades defensivas y de operaciones multidominio. • Definición de estructura y fuerza requerida.	• Innovadora, polivalente, interoperable en ejercicios multinacionales con alcance continental. • Referente regional: consolidación de relacionamiento estratégico. • Capacidades para disuadir y enfrentar amenazas multidominio.	• Innovadora, polivalente, interoperable en operaciones multinacionales con alcance global. • Líder preferente regional, para contribuir a la seguridad y la asistencia humanitaria hemisférica. • Capacidades disuasivas reales, permanentes y sostenibles para enfrentar las amenazas multidominio.

Fuente: FAC (2020).

El Plan de Desarrollo Prospectivo de la Fuerza Aérea Colombiana incluye un programa de transformación organizacional orientado a mejorar los resultados de los procesos e impulsar capacidades que permitan identificar oportunidades de mejora (FAC, 2019a, p. 23). La nueva proyección institucional dispone que para 2042 se dará respuesta a las transformaciones, los riesgos y las amenazas que trae la globalización, desde el modelo de planeación y desarrollo de capacidades de la Fuerza Pública DOMPI (por las iniciales de Doctrina, Organización, Material y Equipo, Personal e Infraestructura).

La transformación organizacional y operativa de la FAC da cuenta del compromiso con la seguridad del país y con la innovación, que actualmente exigen implementar nuevas dinámicas organizacionales y tecnológicas que respondan a los nuevos modelos de seguridad multidimensional.

De esta forma, la FAC, desde sus capacidades, aporta principalmente al logro de los objetivos de las áreas misionales del sector defensa expuestas en la Resolución 0201 de 2021 (Ministerio de Defensa Nacional, 2021), como: defensa nacional, seguridad pública, cooperación internacional y diplomacia para la defensa y seguridad y, finalmente, gestión y apoyo institucional. Integra también las áreas misionales de contribución, como gestión de riesgo y desastres, protección de recursos naturales y del medio ambiente, y desarrollo del país. Lo

anterior, con la finalidad de resaltar la respuesta oportuna frente a las amenazas emergentes, tal como se presenta en la tabla 2.

Tabla 2. *Contribución del poder aéreo, espacial y ciberespacial y las capacidades de la Fuerza Aérea Colombiana frente a las amenazas emergentes*

Áreas misionales	Contribución de la FAC desde las capacidades	Amenazas emergentes
Defensa nacional y seguridad pública	Contribución Mantener la soberanía, la integridad territorial y el orden constitucional, frente a las amenazas internas y externas (FAC, 2020, pp. 2-17).	• Terrorismo. Narcoterrorismo Problemas tribales, étnicos y políticos internos. • Tráfico ilícito de armas. • Crimen cibernético. • Lavado de activos.
	Capacidades • Operaciones de patrulla aérea, escolta aérea, interdicción y ataque estratégico. • Apoyo aéreo cercano. • Inteligencia aérea. • Vigilancia y reconocimiento que promuevan la neutralización o la destrucción de los centros de gravedad del enemigo (FAC, 2020, pp. 2-17).	
Contribución a la gestión de riesgos de desastres	Contribución Apoyo al Sistema Nacional de Gestión de Riesgo y Desastres (SNGRD) (FAC, 2020, pp. 2-17).	Catástrofes naturales
	Capacidades • Transporte de ayuda humanitaria. • Extinción de incendios. • Acercamiento a las regiones más apartadas. • Operaciones de búsqueda y rescate en diferentes emergencias (como accidentes aéreos), evacuación y transporte aeromédico. • Apoyo a la población en eventos como bloqueos viales y extinción de incendios (FAC, 2020, pp. 2-17).	

Áreas misionales	Contribución de la FAC desde las capacidades	Amenazas emergentes
Cooperación internacional	**Contribución** Desarrollo de operaciones combinadas; fortalecimiento de los sistemas de defensa de otros países, para contribuir a la lucha contra amenazas transnacionales (FAC, 2020, pp. 2-18).	• Crimen organizado internacional • Migración masiva y descontrolada. • Problema global de las drogas.
	Capacidades • Participación en encuentros internacionales que permitan fortalecer el cumplimiento de la misión. • Establecimiento de acuerdos en áreas como operaciones logísticas, seguridad operacional, seguridad y defensa de bases aéreas, defensa aérea, ayuda humanitaria, atención de desastres, asuntos espaciales, ciberdefensa y lucha contra amenazas transnacionales (FAC, 2015, citada en FAC, 2020, pp. 2-18)	
Contribución a la protección de los recursos naturales y del medioambiente	**Contribución** A la defensa, la vigilancia y la protección del agua, la biodiversidad y del medio ambiente, como activos estratégicos de la nación (FAC, 2020, pp. 2-18).	• Degradación del medioambiente. • Minería ilegal/crimen de la vida salvaje y forestal
	Capacidades • Liderar proyectos encaminados a: • Ahorro, protección y uso eficiente de recursos naturales. • Gestión de residuos sólidos y saneamiento básico.	
Contribución al desarrollo del país	**Contribución** Consolidación y desarrollo del territorio y de la población, a través de la acción unificada que contribuya al logro de los fines del Estado (FAC, 2020, pp. 2-18).	• Pobreza. • Crisis económicas. • Epidemias
	Capacidades • Llegar a poblaciones vulnerables del país. • Jornadas de apoyo al desarrollo y asistencias humanitarias (FAC, 2019 citada en FAC, 2020, pp. 2-18).	

Áreas misionales	Contribución de la FAC desde las capacidades	Amenazas emergentes
Gestión y apoyo institucional	**Contribución** Promover el desarrollo de la industria (FAC, 2020, pp. 2-18).	Ataques a la seguridad cibernética.
	Capacidades • Desarrollar proyectos de I + D + I para potencializar las capacidades distintivas que permitan proteger los dominios aéreo, espacial y ciberespacial.	

Fuente: FAC (2020).

Ahora bien, para aclarar más la evolución de la FAC, la institución hizo un planeamiento de la estrategia a mediano plazo, el cual puede incluir la actualización de planes, documentos anteriores y el concepto operacional. Por lo tanto, y para esclarecer la evolución de la FAC con respecto a la multidimensionalidad de la seguridad, se hará una comparación de la evolución y los cambios de acuerdo con la dinámica del conflicto, las políticas de gobierno y el pensamiento estratégico institucional en cada momento.

En consecuencia, la FAC asume nuevos roles en el contexto y promueve acciones de respuesta inmediata y decisiva frente a los cambios, los retos y las amenazas que podrían afectar la defensa y seguridad del país, y que influyen, por ende, en el proceso de planeamiento por capacidades (FAC, 2020) y contribuyen, de forma positiva e innovadora, a la seguridad del país (Benavides et al., 2019).

Conclusiones

Colombia ha tenido una profunda transformación en su forma de ver la seguridad y en cuanto a la formulación de las políticas que la regulan, en concordancia con las condiciones históricas que surgen en cada etapa histórica. Así, en el país ha existido un desarrollo que ha permitido a la seguridad y sus políticas reguladoras enfocarse en el ejercicio del poder en el Estado, ocasionado, en gran medida, por circunstancias únicas, como la amplia separación entre asentamientos humanos y la difícil geografía del territorio colombiano, el constante antagonismo entre las élites políticas o la profunda desigualdad que se ha palpado a lo largo del tiempo. Este desarrollo en el cambio de la concepción, por tanto, ha permeado la forma de llevar a cabo la guerra en Colombia, y derivado, desde lo

político, en elementos clave para el ejercicio del monopolio del poder; entre estos, el tamaño de la Fuerza Pública (EJC, ARC, FAC y Policía), las estrategias militares plasmadas en los planes de guerra e, incluso, las tácticas operacionales de las tropas emplazadas en el terreno.

Tal cambio ha llegado al punto en el que Colombia ha podido concebir su propia seguridad desde el enfoque de la seguridad multidimensional, y alejarse así de la clásica concepción de la seguridad nacional utilizada durante el siglo XX. Este nuevo enfoque ha hecho que se advierta la presencia de nuevas amenazas, alejadas de las de tipo tradicional con las que se ha estado luchando desde inicios del siglo XIX. Aquellas amenazas no tradicionales y estructurales han sido incluidas como elementos clave en las nuevas políticas de seguridad y defensa de los más recientes gobiernos, como elementos que aportan a la integralidad de la seguridad del país y garantizan a los colombianos su protección ante aquello que podría afectar el desarrollo normal de su vida, como la pobreza y las afectaciones medioambientales, entre muchos otros.

Al mismo tiempo, este nuevo enfoque de la seguridad multidimensional ha permitido un cambio profundo en los roles de las FF. MM. de Colombia. Anteriormente, basados en las conceptualizaciones de las teorías clásicas, como las de Nicolás Maquiavelo, la Fuerza Armada era, simplemente, el ejercicio legítimo de la fuerza, ya fuese contra un enemigo externo o a fin de conseguir el orden público legítimo; sin embargo, en la actualidad, la introducción de aquellas nuevas amenazas, distinguidas desde la lupa de la seguridad multidimensional, ha permitido que las FF. AA. aumenten sus actividades, para llegar a la realización de actividades que hoy son conocidas como *acción integral*: el acceso a lugares donde han ocurrido graves desastres naturales para ayudar a la población afectada, la eliminación y la reducción de economías ilegales como el narcotráfico, la lucha contra epidemias y otras afectaciones a la salud de la población, entre otras. Lo anterior ha significado un cambio en el paradigma de la utilidad de las FF. MM.; especialmente, en un momento de la historia en el que la guerra entre Estados no es el principal protagonista de las relaciones internacionales.

Entre dichas fuerzas, la FAC ha tenido un cambio en el accionar del poder aéreo y la evolución de sus capacidades tecnológicas a favor de la seguridad nacional. La FAC, nacida como parte integral del EJC, lleva más de 100 años otorgando seguridad en el cielo a los colombianos, ante cualquier amenaza nacional o internacional, y en tal medida, ha logrado adaptarse de forma eficiente; en especial, implementando la modernización tecnológica de las FF. MM. de

comienzos del siglo XX, para adaptarse a las amenazas tradicionales, ya fuese con la realización de acciones de interdicción aérea en contra de aeronaves de países ajenos en territorio nacional o el ejercicio del poder aéreo en operaciones contraguerrilla. Entre estas últimas, una de las más conocidas fue la Operación Vuelo de Ángel, en 1998.

Esta evolución no ha sido ajena a la evolución de la concepción de seguridad hacia la multidimensionalidad. La FAC ha logrado captar en sus áreas misionales y en sus planes estratégicos elementos del nuevo enfoque para el ejercicio de sus capacidades aéreas y la lucha contra las amenazas emergentes, lo que ha abierto un nuevo rumbo a los roles de la FAC en la perspectiva de la seguridad en Colombia. Esto último garantiza que el país logre ejercer el desarrollo del poder aéreo en entendimiento de su nueva función; sobre todo, en un proceso histórico clave como el posconflicto, así como la lucha contra los nuevos fenómenos de COT, los desastres naturales y la salvaguarda de la ciudadanía colombiana y su libertad.

Por esto, se puede afirmar que la FAC, a través de la acción unificada, ha construido espacios de acercamiento con las comunidades, gracias a sus capacidades en la atención de desastres, y su oportuna atención frente a la crisis causada por la pandemia, lo cual se ve reflejado en mejorar la calidad de vida de la comunidad y fortalecer los lazos de confianza entre la sociedad y la institución para garantizar una mayor gobernabilidad.

Referencias

Afanador-Llach, M. J. (2018). Una república colosal: la unión de Colombia, el acceso al Pacífico y la utopía del comercio global, 1819-1830. *Anuario Colombiano de Historia Social y de la Cultura, 45(2)*, 35-63. https://doi.org/10.15446/achsc.v45n2.71026

Atehortúa, A. L., & Vélez, H. (1994). Regeneración y Ejército: el mecanismo de la fuerza. En A. L. Atehortúa & H. Vélez, *Estado y Fuerzas Armadas en Colombia (1886-1953)* (pp. 25-54). Tercer Mundo Editores, Pontificia Universidad Javeriana, Cali.

Barrero-Barrero, D., Baquero, F., & Gaitán, A. (2018). 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, 13*(1), 72-81. https://doi.org/10.18667/cienciaypoderaereo.587

Barrero-Barrero, D., & Olarte, J. (2020). Bajo la protección de las aves: superioridad aérea en las guerras y la campaña aérea moderna. En D. Barrero-Barrero (Ed.), *Superioridad aérea: una comprensión amplia de enfoque nacional* (pp. 65-102). Planeta.

BC Noticias. (2021, 8 de julio). Presidente Duque destaca Operación San Roque y la califica como el mayor despliegue humanitario de la historia del país. https://n9.cl/6dpmp

Benavides, E., Mezú, R., & Ortiz, A. (Eds.). (2019). *Victorias desde el aire: la Fuerza Aérea Colombiana y el término del conflicto armado* (4.a edición). Grupo Editorial Ibáñez.

Bock, J. (2019). La comunicación en la frecuencia de la guerra. En J. Bock (Ed.), *Periodismo roto: viaje por las grietas de la información en Colombia* (pp. 23-29). Fundación para la Libertad de Prensa.

Bushnell, D. (1996). *Colombia. Una nación a pesar de sí misma*. Planeta.

Calvo, J. L. (2013). La evolución de la estrategia militar desde Clausewitz hasta la Segunda Guerra Mundial. En J. Jordán (Comp.), *Manual de estudios estratégicos y seguridad internacional* (pp. 89-116). Plaza y Valdés Editores.

Carvajal, J. (2008). Seguridad humana, en el contexto de la lucha contra el terrorismo. *Novum Jus, 2*(1), 205-234. https://repository.ucatolica.edu.co/handle/10983/17729

Castillo, J. (2019). *Nuevos roles de las fuerzas armadas ante las nuevas amenazas trasnacionales y de seguridad ambiental* [Tesis de especialización, Universidad Militar Nueva Granada]. https://n9.cl/4r85s

Centro de Estudios Históricos del Ejército. (2007). *Historia militar del Ejército de Colombia*. Ejército de Colombia.

Cimadevilla, J. (2019). *De viejas cicatrices a nuevas heridas*. Planeta.

Conde, J. (2016). Pioneros y precursores del poder aéreo en Colombia. Alberto Pauwels Rodríguez. En A. Gaitán (Comp.), *Pensadores, pioneros y precursores del poder aéreo* (pp. 155-163). Editorial Escuela Superior de Guerra.

Constitución Política de Colombia. [Const.]. Julio 7 de 1991. (Colombia).

Deas, M. (2017). Las fuerzas del orden. En M. Deas (ed.), *Las fuerzas del orden y once ensayos de historia de Colombia y las Américas* (pp. 17-46). Taurus.

De la Cruz, G. (1978). Operaciones aeromóviles de contra-guerrillas. *Revista de las Fuerzas Armadas, 30*(88), 25-43. https://issuu.com/esdeguecol/docs/88

Domínguez, J. F. (2018). Capítulo IV. Base Escuela Ernesto Samper Pizano 1935-1955. En J. F. Domínguez, *Historia del Desarrollo Educativo de la Escuela Militar de Aviación "Marco Fidel Suarez". Expresión del proceso de modernización en Colombia (1933-2018)* (pp. 40-42). https://issuu.com/publicientificasemavi/docs/ilovepdf_merged

Esquivel, R. (2010). *Neutralidad y orden. Política exterior y militar en Colombia, 1886-1918*. Pontificia Universidad Javeriana.

Esquivel. R. (2015). La Fuerza Aérea Colombiana y el cese del conflicto armado (1998-2015). *Revista Científica General José María Córdova, 14*(17), 377-401. https://tinyurl.com/5fyebmyz

Esquivel, R. (2019). Fuerza Aérea y conflicto en el Caribe colombiano, 1980-2010. *Ciencia y Poder Aéreo, 14*(2), 122-139. https://doi.org/10.18667/cienciaypoderaereo.637

Font, T., & Ortega, P. (2012). Seguridad nacional, seguridad multidimensional, seguridad humana. *Papeles de relaciones ecosociales y cambio global*, (119), 161-172. https://n9.cl/8oac5

Fuerza Aérea Colombiana [FAC]. (2003). *Plan Estratégico Institucional 2003-2010*. Ministerio de Defensa Nacional.

Fuerza Aérea Colombiana [FAC]. (2006). *Plan Estratégico Institucional 2006-2019*. Ministerio de Defensa Nacional.

Fuerza Aérea Colombiana [FAC]. (2011). *Plan Estratégico Institucional 2011-2030*. Ministerio de Defensa Nacional.

Fuerza Aérea Colombiana [FAC]. (2019a). *Análisis Prospectivo 2022-2030-2042*. FAC.

Fuerza Aérea Colombiana [FAC]. (2019b). *Publicaciones. Poder aéreo, poder transformador*. Fuerza Aérea Colombiana. https://n9.cl/pd9zsv

Fuerza Aérea Colombiana [FAC]. (2020). *Publicaciones. Estrategia para el desarrollo aéreo y espacial de la Fuerza Aérea Colombiana 2042*. Fuerza Aérea Colombiana. https://www.fac.mil.co/sites/default/files/2021-04/edaes.pdf

Fuerza Aérea Colombiana [FAC]. (2021, 10 de agosto). *Conózcanos*. Fuerza Aérea Colombiana. https://tinyurl.com/5daza7r7 García, J. (2016). *Nuevas amenazas y transformación de la defensa: el caso de Latinoamérica*. Instituto Universitario General Gutiérrez Mellado. https://tinyurl.com/yc2pnbrh

Hernández, D. (2017). Armas aire-superficie en la Fuerza Aérea Colombiana. *Air & Space Power Journal, 29*(3), 80-90. https://n9.cl/g9ygda

Hernández, D. (2020). La aviación del Ejército colombiano. Inicio de la aviación militar en Colombia. *Revista Fuerza Aérea-EUA*, segunda edición, 43-58. https://tinyurl.com/56z7hzx7

Junta Interamericana de Defensa. (2021). *Amenazas emergentes*. https://www.jid.org/?page_id=710

Leal, F. (2003). La doctrina de seguridad nacional: materialización de la Guerra Fría en América del Sur. *Revista de Estudios Sociales*, (15), 74-87. https://revistas.uniandes.edu.co/doi/pdf/10.7440/res15.2003.05

Lind, W., & Thiele, G. (2015). *4th Generation Warfare Handbook*. Castalia House.

Macisaac, D. (1992). Voces desde el azul del cielo: los teóricos del poder aéreo. En P. Paret (Ed.), *Creadores de la estrategia moderna: Desde Maquiavelo a la Era Nuclear* (pp. 639-664). Ministerio de Defensa de España, Secretaría General Técnica.

Maquiavelo, N. (1520/2011). *El arte de la guerra*. Ediciones Leyenda.

Meza, A. (2016). Pensadores universales del poder aéreo. Giulio Douhet. En A. Gaitán (Comp.), *Pensadores, pioneros y precursores del poder aéreo* (pp. 19-26). Editorial Escuela Superior de Guerra.

Ministerio de Defensa Nacional. (2011). *Política Integral de Seguridad y Defensa para la Prosperidad*. https://n9.cl/0ne5y

Ministerio de Defensa Nacional. (2019). *Política de Defensa y Seguridad (PDS)*. https://n9.cl/fllc

Ministerio de Defensa Nacional. (2021). *Resolución 0201 del 5 de febrero de 2021, por la cual se definen y adoptan las Áreas Misionales del Sector Defensa*. https://tinyurl.com/4sjr9apm

Montgomery, B. (1969). *Historia del arte de la guerra*. Aguilar.

Nova, M. (2019). La historia de Colombia es una historia de sufrimientos. En M. Nova (Ed.), *Memorias militares* (pp. 125-163). Planeta.

Pardo, R. (2008). *La historia de las guerras*. Ediciones Zeta.

Parra, B. (1998). Vida, pasión y muerte de Scadta. Origen y desarrollo de la aviación en Colombia. *Innovar* (12), 93-116. https://tinyurl.com/yc3ey5yd

Pérez, J. (2016). El conflicto con el Perú 1932-1933 y el inicio de la política de industrialización en Colombia. *Revista Estudios en Seguridad y Defensa, 11*(21), 27-43. https://doi.org/10.25062/1900-8325.49

Resdal. (2016). *Colombia. Atlas Comparativo de la Defensa en América Latina y el Caribe*. https://www.resdal.org/assets/atlas_2016_esp_14.pdf

Rodríguez, S. (2006). *La influencia de los Estados Unidos en el Ejército colombiano, 1951-1959*. La Carreta Editores y Universidad Nacional de Colombia.

Rosanía, N., Sánchez, D., & López, G. (2017). Rupturas y continuidades de la seguridad y defensa en Colombia. De la seguridad nacional a la seguridad multidimensional. En C. Álvarez (ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 85-144). Escuela Superior de Guerra.

Soler, F. (1988). La aviación militar en Colombia. *Revista de las Fuerzas Armadas, 43*(127), 181-189. https://issuu.com/esdeguecol/docs/127

Sotelo, A. (2016). Asher Lee. En A. Gaitán (Comp.), *Pensadores, pioneros y precursores del poder aéreo* (pp. 37-44). Escuela Superior de Guerra.

Ugarte, J. (2001). *Los conceptos defensa y seguridad en América Latina; Sus peculiaridades respecto de los vigentes en otras regiones, y las consecuencias políticas de tales peculiaridades*. Congreso LASA.

Ugarriza, J., & Pabón, N. (2018). *Militares y guerrillas. La memoria histórica del conflicto armado en Colombia desde los archivos militares, 1958-2016* (2.a ed.). Editorial Universidad del Rosario.

Useche. F. (2019). *Sentido de la formación en la Escuela Militar de Aviación "Marco Fidel Suárez". Una mirada desde lo militar, lo aeronáutico y lo profesional* [Tesis de Maestría, Universidad San Buenaventura]. https://tinyurl.com/58bdhu4v

Valencia, A. (1964). Defensa nacional y guerra revolucionaria. *Revista de las Fuerzas Armadas, 8*(24), 393-400. https://issuu.com/esdeguecol/docs/24

Van Creveld, M. (2015). *A history of strategy: from Sun Tzu to William S. Lind*. Castalia House.

Vargas, A. (2008). La lenta marcha en el siglo XX hacia un ejército profesional moderno en Colombia. En C. Torres del Río T S. Rodríguez (Eds.), *De milicias reales a militares contrainsurgentes. La institución militar en Colombia del siglo XVIII al XXI* (pp. 299-336). Editorial Pontificia Universidad Javeriana.

Villalobos, J. (1993). Historia de la Fuerza Aérea Colombiana. En A. Valencia, *Historia de las Fuerzas Militares de Colombia* (tomo 5). Planeta.

Capítulo 2

Contexto global contemporáneo de cara a las amenazas, los nuevos retos y los desafíos multidimensionales*

DOI: https://doi.org/10.25062/9786287602106.02

Carlos Andrés Herrera Ibagos
David Barrero Barrero
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo tiene como propósito exponer la complejidad de las relaciones internacionales respecto a los intereses comunes en materia de seguridad global, regional y local, así como problematizar la posibilidad de enfrentar las amenazas a la seguridad de una forma cooperativa bajo un mismo ideal común, y dar una respuesta efectiva y definitiva en materia de negación, contención y anticipación del problema de la seguridad y defensa de las naciones. El capítulo caracteriza las amenazas, los nuevos retos y los desafíos multidimensionales de la seguridad y el orden internacional, en el contexto contemporáneo global y regional.

Palabras clave: Amenazas, poder aéreo, espacial y ciberespacial, seguridad multidimensional, relaciones internacionales.

* 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.

Carlos Andrés Herrera Ibagos
Teniente Coronel de la Fuerza Aérea Colombiana. Piloto militar y administrador aeronáutico. Profesional en Relaciones Internacionales y Estudios Políticos de la Universidad Militar Nueva Granada. Magister en Seguridad Operacional de la Escuela de Posgrados de la Fuerza Aérea Colombiana. Magister en Seguridad y Defensa Nacionales de la ESDEG. Contacto: carlos.herrerai@fac.mil.co

David Barrero Barrero
Coronel de la Reserva Activa de la Fuerza Aérea Colombiana. Piloto militar y administrador aeronáutico. Master of Science in Inter-American Defense and Security, del Colegio Interamericano de Defensa. Candidato a Doctor en Bioética en la Universidad Militar Nueva Granada. Docente e investigador junior MinCiencias del Grupo Masa Crítica, de la ESDEG. ORCID: https://orcid.org/0000-0003-0412-1371 - Contacto: david.barrero@esdeg.edu.co

Citación APA: Herrera Ibagos, C. A., & Barrero-Barrero, D. (2022). Contexto global contemporáneo de cara a las amenazas, los nuevos retos y los desafíos multidimensionales. En F. Baquero Valdés (Ed.), *Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano* (pp. 63-108). https://doi.org/10.25062/9786287602106.02

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

Los seres humanos hemos padecido la violencia desde la época de nuestros antepasados prehistóricos, en lo que desde entonces se ha constituido en parte de la propia naturaleza humana, y se ha potencializado a lo largo de la historia dependiendo del entorno, el deseo de poder, el odio, la religión y, en general, una larga lista de motivos, que, en realidad, no tienen justificación, vistos desde la ética por el respeto a la vida y la dignidad humana. Hoy, la guerra, el terrorismo y todas las amenazas contenidas en el COT son las grandes catástrofes que agobian la existencia pacífica del género humano y de la naturaleza en general, las cuales han evolucionado a tal punto que ponen en riesgo la seguridad global.

El presente capítulo tiene por objetivo establecer la proyección de empleo del poder aéreo, espacial y ciberespacial para combatir y contener las amenazas con los nuevos desafíos multidimensionales, que enfrenta el Estado colombiano para garantizar la seguridad y defensa nacional. Para llevar a cabo lo planteado, se usará el método analítico cualitativo de investigación, por medio de la técnica de revisión y análisis documental, para dar cuenta de la proliferación de amenazas a la seguridad global, a fin de llegar a los retos y los desafíos contemporáneos.

Lo anterior, considerando de vital interés los dilemas que enfrenta la sociedad del siglo XXI respecto a la seguridad, donde el orden mundial y las relaciones internacionales son imprescindibles para comprender la evolución de las amenazas tradicionales y las nuevas amenazas que enfrentan los Estados, y de ahí, entender los problemas de seguridad con los que convive la humanidad, a fin de buscar soluciones para negar, contener y anticipar estas amenazas.

Al respecto, cabe destacar que finalizada la Primera Guerra Mundial "surgió por primera vez el término de 'orden mundial' en el Congreso de Estados Unidos

(EE. UU.) y en el Tratado de Versalles por parte del presidente norteamericano Woodrow Wilson" (Blin & Marín, 2013, p. 216). En ese sentido, y a partir de lo mencionado, debe entenderse que *nuevo orden mundial* se emplea para describir el papel que juegan las potencias globales en el predominio del sistema internacional en los aspectos económico, político, militar y social, bien sea por hechos violentos, como la guerra interestatal, o por la guerra que pelean algunos países colectivamente en la contemporaneidad en contra del terrorismo.

Así las cosas, desde la creación de los Estados, las guerras han estructurado el orden mundial, donde se han rediseñado fronteras y se han creado nuevos territorios sobre lo conquistado o lo arrebatado en una confrontación, y se han impuesto nuevas formas culturales y religiosas a su paso. En ese orden de ideas, la guerra y la paz terminaron siendo equivalentes alrededor de la vida humana, o como lo describe Fernández-Montesinos (2011), "la guerra como la paz tienen la misma finalidad y, por lo tanto, no son ni pueden ser conceptos antinómicos" (p. 21), razón por la cual el siglo XX ha sido un periodo en el que las guerras, los conflictos y, en general, las amenazas, llevaron a buscar soluciones en la seguridad nacional, la seguridad cooperativa y la defensa colectiva, entre muchas más, las cuales se plantearon por la falta de alcance del significado simple de *seguridad*.

Para el desarrollo del tema planteado, se proponen tres apartados. En el primero se examina el ambiente global y regional de amenazas multidimensionales que afectan la seguridad y defensa nacional. Y para ello, se tendrá en cuenta la importancia de las guerras como los sucesos de mayor impacto en el orden mundial. Dicho apartado abarca los conflictos más relevantes del siglo XX, así como el ataque a las Torres Gemelas y el Pentágono, en el llamado 9-11, donde se pone en contexto lo que se define como el orden mundial, desde la perspectiva del neorrealismo como pensamiento de las relaciones internacionales.

Lo anterior, debido a que "el neorrealismo se representa en una circularidad tautológica de la estructura del sistema internacional como variable independiente y la estabilidad del sistema internacional como variable dependiente" (Vargas, 2010, p. 120; Waltz, 1988, p. 619), lo que implica un enfoque en el equilibro de poderes en el contexto global, donde los Estados buscan la supervivencia generando una posibilidad de análisis a través de los conflictos o las guerras que se han vivido.

En el segundo apartado se propone la categorización de las nuevas amenazas de mayor impacto que afectan el mundo contemporáneo, a partir de la Declaración de la Seguridad de las Américas de 2003 y 2020, de la OEA, donde

fue posible realizar un análisis comparativo con otras organizaciones, como la OTAN y la ONU; en esta última se incluye a la UNODC, donde los resultados mostraron similitudes y acepciones en algunos casos, así como el aumento de amenazas desde finales del siglo XX, pero, en definitiva, una mutación de nuevas amenazas con transnacionalización global.

Por último, se evalúan los sucesos de mayor relevancia de los siglos XX y XXI, los cuales promovieron un cambio en el orden mundial en el área de las relaciones internacionales y la generación de nuevas amenazas del mundo contemporáneo, lo que permite proponer los posibles retos del mundo, en el marco de la seguridad, para las próximas décadas de la presente centuria, aspecto pertinente para desarrollar un análisis prospectivo a las estrategias de seguridad de los Estados, para combatir los futuros peligros que empiezan a gestarse en el ambiente ciberespacial. Al final, se plantean las conclusiones resultado de la investigación.

Ambiente global y regional de amenazas multidimensionales que afectan la seguridad y defensa nacional

Este apartado tiene como objeto hacer una evaluación del escenario mundial y el nuevo orden contemporáneo, a partir de los hechos históricos del final del siglo XX que generaron un impacto en las relaciones internacionales, con el fin de verificar los aspectos clave que hoy en día están generando un hito en materia de seguridad, lo cual lleva a cuestionar acerca de cuáles serán las tendencias de los Estados para alcanzar sus intereses y, al mismo tiempo, mantener el equilibrio mundial.

Desde el recuento de la historia, las dos guerras mundiales se convirtieron en los puntos de inflexión para explicar muchos cambios sociales de la humanidad (Bouthoul, 1971; Burkett, 2020); por tanto la guerra puede ser considerada el acontecimiento de mayor impacto en la historia de la humanidad, la cual establece por sí sola las variables del desarrollo y la evolución del ser humano, donde la búsqueda del interés propio y la misma naturaleza del individuo lo han llevado a involucrarse en guerras que, en definitiva, conllevan resultados trágicos para comunidades enteras que han padecido los males de la guerra. A pesar de esto, el mismo ser humano ha demostrado su inmenso poder de sobreponerse a los males que él mismo desarrolla.

Y es que a lo largo del recorrido histórico de la conformación entre los Estados, la necesidad de mayor poder es una de las características por las cuales se llega a ese tipo de confrontación, por lo cual los propios oponentes plantean, según sus necesidades y sus ambiciones, los objetivos de la guerra que van a emprender. Por lo tanto, en todas las guerras —incluso desde "las guerras viejas (desde el siglo XVII- Finales del siglo XX) […] los Estados tenían la necesidad de consolidar sus fronteras y posteriormente buscaban imponer su ideología" (Kaldor, 2012, p. 13).

Esto último deja en evidencia que un motivo tradicional para luchar en un campo de batalla contra otro, considerado enemigo, era la expansión de territorio, lo cual llevaba a los Estados a tener una confrontación bélica, que tradicionalmente traía como consecuencia la muerte de miles de seres humanos. Lo anterior se alinea con Clausewitz (2005), quien concebía la guerra como "un acto de violencia para obligar al contrario a hacer nuestra voluntad" (p. 34). A pesar de esto, no se puede ni debe considerar imperativa la justificación del porqué de una guerra como fin para cumplir los intereses de un Estado. En tal sentido, las guerras son acontecimientos lamentables, y con los cuales la cultura humana ha aprendido a convivir, aun sabiendo que para lograr la paz entre dos o más actores se requiere una colectividad común.

Por lo anterior, se han propiciado diferentes tratados y alianzas, para evitar, de alguna manera, reducir la cadencia de guerras a lo largo de la historia. Sin embargo, estos acuerdos no han tenido el impacto deseado, debido a las diferencias de intereses por parte de los involucrados. Un ejemplo de lo anterior fue cuando "el 18 de mayo de 1898, por primera vez en la Haya, diferentes Estados se congregaron para buscar la paz, pero años más tarde se generarían las guerras mundiales" (Bouthoul, 1971, p. 113), lo cual demuestra que, para algunos, la guerra sigue siendo la solución cuando no se logran los objetivos de un actor dominante.

De igual forma, el siglo XX fue un periodo de guerras importantes, pero, más que todo, funestas, como la Primera Guerra Mundial (I GM) (1914- 1918), la Segunda Guerra Mundial (II GM) (1939-1945), la primera guerra Árabe-Israelí (1948), la guerra de Corea (1950-1953), la guerra de Vietnam (1955-1975), la guerra de los Seis Días (1967) y la guerra del Golfo (1990-1991), entre otras (Álvarez, 2018; Uribe, 2013). En cada una de ellas, autores y expertos plantearon un nuevo orden mundial, a partir de los hechos, la tecnología militar empleada, el nivel de violencia, los territorios comprometidos y hasta la cantidad de vidas humanas

perdidas. Lo cierto es que las guerras, por su impacto y su trascendencia, hacen parte de los procesos aceleracionistas y desincronizados de la sociedad contemporánea (Rosa, 2011), debido, entre otras, a la tecnificación humana en doble sentido: mejorar los procesos de la vida, o afectarlos y ponerlos en peligro.

Respecto a la marcada violencia propia de los seres humanos, tratada líneas arriba, Keegan (2014) pone en contexto la realidad humana de la violencia y el desprecio por la vida como formas de relacionamiento entre los hombres como parte de su naturaleza; de hecho, afirma que "la antropología nos dice, y la arqueología nos indica, que nuestros antepasados civilizados eran sanguinarios, en tanto el psicoanálisis trata de persuadirnos de que en todo hombre anida un salvaje en lo más profundo de su ser" (p. 31).

En otro sentido, las dos guerras mundiales y la consecuente Guerra Fría, así como la carrera nuclear y espacial entre estadounidenses y soviéticos, la caída del Muro de Berlín y, finalmente, la guerra del Golfo, a finales del siglo XX, trazaron en esa centuria una lucha por el dominio y el liderazgo mundiales, que terminaron en manos de Estados Unidos. Estos hechos, además de los planteados previamente, marcaron una mayor importancia de lo que define la seguridad nacional, basada en los intereses nacionales en nombre de los que se pretende, desde entonces, llevar a cabo una guerra; de hecho, en la actualidad, y tras la desterritorialización del terrorismo con los hechos del 9-11, se amplió aún más el alcance de este término, al punto de lanzarse operaciones aliadas en territorios extranjeros, buscando neutralizar la nueva amenaza del siglo XXI.

Además de todo lo anterior, la guerra como amenaza mutó a una nueva dimensión más compleja; así, los campos de batalla de los conflictos internacionales se llevaron al interior de los países. Además de la guerra en el sentido tradicional entre los Estados, las guerras intraestatales o los conflictos internos se llevan a cabo en una mayor diversidad de formas, tales como el terrorismo, la violencia y la persecución por razones de género, las guerras civiles, el reclutamiento forzoso con fines terroristas —especialmente, de niños— y la desaparición de seres humanos, entre muchas más, que ponen en riesgo los intereses nacionales en algunas naciones (Pozo, 2010).

Precisamente, fue el siglo XX el que dio origen a nuevos ambientes para llevar a cabo las guerras, pues a lo largo de este se generaron otras formas de combate mucho más letales y tecnológicamente más efectivas, lo que puso a prueba a los actores del orden internacional en los debates de la guerra justa por la naturaleza ofensiva o defensiva, en la "agresión o la trasgresión de las normas

que hace el enemigo" (Fernández-Montesinos, 2011, p. 95). Por lo tanto, el siglo XX estuvo marcado por las guerras tradicionales llevadas a cabo en los escenarios tridimensionales de tierra, mar y aire (Álvarez, 2018); fue, precisamente, este último el que le imprimió un mayor papel decisivo a quien lo hubiera desarrollado mejor estratégicamente. Sin embargo, no son descartables los escenarios espacial y ciberespacial, que potencializan las amenazas y vulneran el derecho internacional a impedir los conflictos, incluyendo los que se llevan a cabo en el interior de los Estados.

Por otra parte, y desde la óptica de los conflictos, la mutación de nuevas generaciones de las guerras, o las llamadas *nuevas guerras*, que plantea Mary Kaldor (2012), generó retos multidimensionales, que debieron involucrar los contextos económico, social, político y cultural, además de lo militar (Organización de Estados Americanos [OEA], 2003), por cuanto los Estados, desde comienzos de siglo, debieron competir en nuevos escenarios, lo que representa mayores desafíos para su futura supervivencia (Álvarez, 2018); aspectos por abordar con posterioridad, incluyendo el análisis consecuentemente de su impacto y de su posible afectación a los Estados.

Bien sea la *polemología de la guerra*, de Bouthoul (1971); la relación de guerra como *conflicto supremo*, de Fernández-Montesinos (2011, p. 19), o la propuesta relacional que hace Keegan con "la economía, la diplomacia y la política" (2014, p. 25), pero que, finalmente, ejecutan seres humanos distintos de políticos y diplomáticos, el hecho es que la guerra ha sido definida en medio de diferencias, similitudes y hasta paradojas, en medio de las relaciones humanas.

Platón mencionó que "la guerra y la paz son etapas sucesivas" (Cataldo, 2008, p. 9) —lo cual da a entender una equivalencia relacional-social en la vida de los seres humanos—. Clausewitz (2005) afirmó que la guerra era "la continuación de la política por otros medios" (p. 46) —y ello sintoniza el entendimiento de muchos autores en torno a tan revolucionaria definición, hasta el momento—. Y John Keegan contrarió todo lo anterior, planteó que "la obligación de la política debe ser la de proveer felicidad y prosperidad a su pueblo, protegiéndolo de cualquier situación de guerra" (Keegan, 2014). Lo cierto es que la guerra tiene mayor afinidad con la política que con la economía, lo social o lo cultural.

De igual forma, la antropóloga Mead definió la guerra como un "conflicto entre dos sociedades movilizadas, en el cual la privación de la vida de personas del bando opuesto no se sanciona, pero si este hecho ocurre entre las filas del mismo bando es tratado como crimen" (Mead, citada por Koprinarov, 2013, p.

145). Por su parte, Koprinarov (2013) considera que "el género humano es el único en el reino animal, que ha superado la barrera biológica que impide convertir los "suyos" en objeto de destrucción" (p. 145), lo cual explica por qué las guerras suceden, y por qué no dejarán de existir ni, menos, de cobrar cada vez más vidas. Por lo tanto, ¿qué cambiaría si los seres humanos no hubiesen inventado la guerra? Quizá, la racionalidad y la inteligencia del hombre serían más brillantes que lo que son.

Desde otra perspectiva, Álvarez, Santafé y Urbano (2018) afirman que la guerra es "una condición de conflicto en el cual puede desenvolverse en acciones violentas o no violentas" (p. 152). Esta definición y las anteriores bien podrían dar por hecho que la guerra *per se* es y seguirá siendo vigente en la vida cotidiana de los humanos y sus relaciones internacionales. Lo cierto es que la guerra jamás será humanamente viable, por cuanto ha sido, quizá, la mayor amenaza a la humanidad desde sus orígenes; una amenaza que se lleva a los hechos por la codicia de poder, por la avaricia o por el odio, como solo algunas de sus muchas naturalezas.

Por otra parte, la II GM forjó una profunda división del poder político y se fundamentó en una estructura bipolar, donde Estados Unidos y la Unión Soviética lucharon, a partir de ahí, y a lo largo de más de 40 años, por el dominio global (Figueroa, 2013). Como consecuencia, se dio inicio a la conocida Guerra Fría, que enfatizó "en pensamientos ideológicos como es el capitalismo y comunismo" (Sanahuja, 2020). Debido a lo anterior, se generó una carrera armamentista, fundamentada en la necesidad de obtener el poder militar a través de la disuasión nuclear, y se incrementó el número de arsenales de este tipo de armamento, y con ello, creció la preocupación mundial por una posible guerra entre las dos potencias del siglo XX, hasta llegar a plantear la guerra total, que, desde el punto de vista de medios —referido a los recursos, especialmente de armas para un conflicto— llevaría a una guerra de carácter ilimitado, y que, en relación con los fines, llevó, por ejemplo, a la lamentable idea de la *mutua destrucción asegurada* (Fernández-Montesinos, 2011, p. 143). Tal situación sigue vigente en pleno siglo XXI.

Para Figueroa (2013), "predominaba una tesis de conflicto latente, que requería de la definición del estatus de cada potencia en el sistema internacional, y de factores concretos que demostraran el poder de cada uno de estos Estados" (p. 21). No obstante, de alguna forma, se generó un equilibrio de poder, donde las fricciones demostraban más una intención *disuasiva*, por encima de la firme intención de ocasionar un conflicto real entre estas dos potencias.

De igual manera, durante el siglo XX ambos países no se enfrentaron directamente en una guerra o un conflicto internacional. Acudieron a terceros países o a naciones satélites de su entorno para llevar a cabo guerras. Se presentaron conflictos como la guerra de Corea, en la que se pusieron en duda el poder y la capacidad tecnológica de Estados Unidos en el ámbito militar (Dos Santos, 2020). Sin embargo, "la estrategia principal utilizada por el país norteamericano con la recuperación de Europa a través del plan Marshall, generó dependencia hacia Estados Unidos, lo cual fortaleció su supremacía global" (Aguilera et al., 2012). De tal manera, Estados Unidos pudo contrarrestar los intereses soviéticos, y así evitar la expansión y una mayor influencia del titán euroasiático en el continente europeo. Lo cierto es que la probabilidad de una guerra de carácter total marcó el temor y la desconfianza en la última parte del siglo XX.

La caída del Muro de Berlín fue el evento de mayor preponderancia en el ámbito de seguridad a finales del siglo XX, ya que se puede considerar un punto de inflexión hacia "otro" y nuevo orden mundial, donde Estados Unidos se convirtió en el país de mayor hegemonía mundial y, por ende, llevó al mundo, inicialmente, a la unipolaridad (Castillo, 2019). Sin embargo, la propia globalización y el acceso al poder —no solo de las naciones, sino de individuos particulares— ha llevado al lógico planteamiento de una multipolaridad en el momento contemporáneo, pues surgen en el entorno internacional nuevos actores con poder; un poder más allá de los Estados.

Según Ramírez y Bolívar (2018), "La caída del Muro de Berlín y el fin de la Guerra Fría, son los hitos que abren la posibilidad histórica de que se entre en una revaluación de las políticas de seguridad hemisférica" (p. 557); de ahí, la imposición de la doctrina Monroe (Buzan & Waever, 2003), por cuanto ese hecho histórico contribuyó a cambios significativos en materia de seguridad, debido a la aparición de nuevas amenazas a la seguridad, como lo planteó la OEA (2003) en su Declaración de las Américas, y las cuales no estaban en el primer punto de la agenda de los países ni de los organismos supranacionales, pues antes era la guerra la que acaparaba la atención mundial, como la amenaza tradicional.

En el mencionado momento histórico, esas nuevas amenazas a la seguridad contribuyeron, quizá, a un nuevo desbalance de poder, debido al terrorismo y al COT. Según Pereyra (2015), "la institucionalización del sistema internacional pasó por tres etapas: una de institucionalización baja (previa a la Segunda Guerra Mundial); otra de institucionalización media (período de Guerra Fría); y una última de alta institucionalización (fin de la Guerra Fría)" (p. 132). Por tal

motivo, conviene enfatizar que la Guerra Fría fue el punto de quiebre en materia de un nuevo orden mundial y de una mayor importancia lograda por las organizaciones internacionales.

En este nuevo reordenamiento mundial de la última década del siglo XX, Estados Unidos intervino en varios asuntos internacionales como "la guerra del Golfo Pérsico (1990-1991), siendo el conflicto más relevante y tradicional de la década" (Aguilera et al., 2012). Y a pesar del liderazgo estadounidense y de su participación activa en organizaciones mundiales como las ONU, la OEA y la OTAN, donde ejerce un papel protagónico en la toma de decisiones colectivas y cooperativas en temas de seguridad, derechos humanos (DD. HH.) y crimen organizado, Estados Unidos es el país víctima de la mayor hecatombe del siglo XXI, cuando fue atacado el 11-09, lo que dejó en entredicho la seguridad del país considerado el más poderoso del mundo. Lo cierto es que el hecho suscitó un nuevo enfoque hacia la seguridad de los Estados (Álvarez & Fernández, 2013).

Por lo tanto, el ataque terrorista en Nueva York en 2001, así como los ocurridos "en Europa el 11 de marzo de 2004 (Madrid) y el 7 de julio de 2005, entre otros más, fueron los acontecimientos que generaron un replanteamiento en materia de seguridad para EE. UU. y Europa" (Font & Ortega, 2012, p. 171). Ello permitió restructurar las nuevas amenazas que afectan el mundo contemporáneo, como la delincuencia organizada trasnacional (DOT), el terrorismo o los ataques a la seguridad cibernética.

El atentado terrorista del 9-11 marcó un hito en la historia estadounidense y en la del mundo. El lamentable acontecimiento fue observado en tiempo real por el planeta, "por cuanto además de tristemente deslumbrar a todos los que vieron caer las torres y con ellas la muerte de muchos ciudadanos del mundo" (Blin & Marín, 2013, p. 296). Se estaba presenciando la desterritorialización del terrorismo, y con ello, un nuevo orden mundial, en el que, sobre todo, Occidente estaría amenazado. De igual manera, este suceso obligó a plantear soluciones, alianzas de carácter internacional dentro de los órganos supranacionales, como en el caso de la seguridad colectiva, mediante la cual se adoptan estrategias como la de coalición internacional en la lucha contra el terrorismo (Chillier & Freeman, 2005).

Es oportuno, entonces, cuestionar si el mundo se hallaba realmente preparado para algo así, si se habría podido anticipar el ataque, o hacia dónde apuntaban los planes de desarrollo de la aviación y la tecnología del momento. Las respuestas se quedan cortas. En tan lamentable momento de la historia, perdieron

la vida demasiados seres humanos de distintas nacionalidades; por lo tanto, fue un ataque contra todos.

A partir del trágico suceso y del éxito que resultaba ser para Al Qaeda, el compromiso frente a la seguridad global requirió un inmediato replanteamiento de estrategias para combatir el terrorismo. Organizaciones internacionales como la OEA definieron las que pasarían a ser consideradas nuevas amenazas a la seguridad a inicios de siglo, con el propósito de que cada uno de los Estados fijara los mecanismos pertinentes a mitigar dichas amenazas (Olaya et al., 2007).

Debido a la aparición de nuevos actores de orden internacional, como lo fue en su momento Al Qaeda, y como los son los demás grupos terroristas que han surgido en el siglo XXI, Olaya et al. (2007) afirman que "el terrorismo se prioriza como la amenaza fundamental contra la cual deben ser orientados los mayores esfuerzos" (p. 10). En consecuencia, las nuevas amenazas, a las que pertenecen el terrorismo, el crimen trasnacional, el narcotráfico y la corrupción, entre muchos más, se volvieron la prioridad en la agenda de los Estados en materia de seguridad, sin que ello quiera decir que las guerras, como amenaza tradicional, ya no existan.

Por otra parte, y planteando una definición de nuevas amenazas, John Griffiths (2009) afirma que:

> Las nuevas amenazas del escenario internacional son un conjunto de fenómenos de diversa naturaleza. Algunos de ellos se expresan violentamente mientras que otros crean las condiciones para que fenómenos violentos se expresen. Dentro de los de expresión violenta encontramos al terrorismo, las organizaciones criminales, el narcotráfico, etc. Dentro de los factores que crean condiciones podemos citar la pobreza, el desempleo, la exclusión social, la corrupción, etc. [Por lo tanto], las nuevas amenazas explotan las debilidades estatales referidas a la falta de gobernabilidad, institucionalidad y presencia estatal en el territorio. Con ellos se quiere enfatizar que las nuevas amenazas encuentran una mayor facilidad para desarrollarse en ambientes o zonas con escasa institucionalidad. (pp. 18-19)

Intereses e interacción de los Estados como impacto de las relaciones internacionales a partir del neorrealismo estructural

Las relaciones internacionales (RR. II.) se hacen importantes, precisamente, al ser constituidas por los Estados y los organismos del sistema internacional,

lo que ha llevado al surgimiento de diversos enfoques como el Realismo, el Neorrealismo y el Constructivismo, entre otros, a lo largo de la historia (Pereyra, 2015). Según Barbe (1989), "el nacimiento de las relaciones internacionales como disciplina está ligado a una preocupación: la existencia de guerras entre Estados" (p. 174). Lo anterior se evidencia con mayor claridad después de la II GM y sus nefastas estadísticas.

Después de la Guerra Fría, uno de los mayores cambios en las RR. II. fue la necesidad de promover un direccionamiento único hacia la seguridad y el mismo comportamiento de los Estados en el sistema internacional, enlazando los poderes económicos y militares de las superpotencias (Schneider, 2015). De igual manera, países como Estados Unidos, China y Rusia, considerados los Estados líderes del sistema internacional (Orozco, 2014), han buscado estrategias para tener un mayor protagonismo en el ámbito de las relaciones internacionales, la globalización y el desespero por el liderazgo en tecnología, y garantizar dicho protagonismo obteniendo información en tiempo real, lo que permite una nueva evolución del concepto *fronteras*.

Según Fazio (2006), en el campo de las relaciones internacionales:

> La identificación de la globalización con el simple aumento de las interconexiones ha servido de nuevo marco legitimador de las tesis realistas y neorrealistas sobre los estudios internacionales, porque como alude a una intensificación de los intercambios entre unidades separadas, permite suponer que la relación entre las unidades (adentro/afuera) sigue siendo más o menos la misma que antes, no obstante, la intensificación experimentada por el proceso globalizador. (p. 58)

En otro sentido, la interacción de los Estados, como en el caso de "la Paz de Westfalia de 1648, el Congreso de Viena de 1815, la Conferencia de Paz de Paris de 1919 y la Conferencia de San Francisco de 1945" (Fernández & Olmedo, 2018, p. 48), además de las conferencias de Yalta y de Potsdam —también en 1945—, contribuyeron a la generación de un nuevo orden mundial. Uno detrás de otro.

En ese sentido relacional, y con el tema de la guerra puesto en la agenda de las naciones, la complejidad de la esta obligó a los Estados a buscar una disciplina que comprendiera los fenómenos y los comportamientos de estos, para evitar los conflictos a gran escala que estaban desequilibrando el orden mundial. Según Blin y Marín, "las relaciones internacionales no designan las relaciones entre naciones sino las relaciones entre los Estados, es decir entre los gobiernos y los altos dirigentes políticos, durante mucho tiempo los monarcas, y no entre

los pueblos" (2013, p. 257), lo cual quiere decir que a través del comportamiento de los Estados se define la armonización del sistema internacional.

En la segunda mitad del siglo XX, como ya se ha mencionado, se fortaleció la disciplina de las relaciones internacionales, y así comenzaron a estructurarse distintos pensamientos o ideologías, las cuales buscaban un entendimiento de lo que estaba sucediendo en la época. Trasladando lo anterior al mundo presente, existen dos pensamientos dentro de la rama de las RR. II. de mayor uso, por su enfoque de cooperación y armonía entre los estados: el *neorrealismo* y el *neoliberalismo* (Patiño, s. f.), como se muestra en la tabla 1.

Tabla 1. *Principales enfoques teóricos de la actualidad en las relaciones internacionales*

Teoría	Prioridad de metas estatales	Énfasis	Anarquía	Cooperación	Expectativas	Beneficios
Neorrealismo	Seguridad	Capacidades	Restricción al comportamiento del Estado	Más difícil de lograrse y mantenerse	Negativas	Relativos
Neoliberalismo	Bienestar Económico	Intenciones	Superable	Regímenes e instituciones la posibilitan	Positivas	Absolutos

Fuente: Patiño (s. f.).

Por otra parte, el neorrealismo, o Realismo estructural, es considerado el principal enfoque usado en RR. II. En dicho modelo, se estudian las capacidades y la interacción de los Estados en un contexto global con características de un mundo anárquico (Hernández, 2008). Este pensamiento o ideología es el que profundiza este documento, por su pertinencia y su impacto en los fines y los medios del Estado. Además, se destaca la relevancia de Kenneth Waltz (citado por Keohane, 1993) mediante de su escrito *Man, the State and War* (p. 65), el cual ha sido estudiado por varios analistas en RR. II., y donde se hace énfasis en tres aspectos fundamentales: la naturaleza del ser humano, la estructura interna del Estado y la actuación de los Estados dentro de un mundo anárquico (Barbe, 1987).

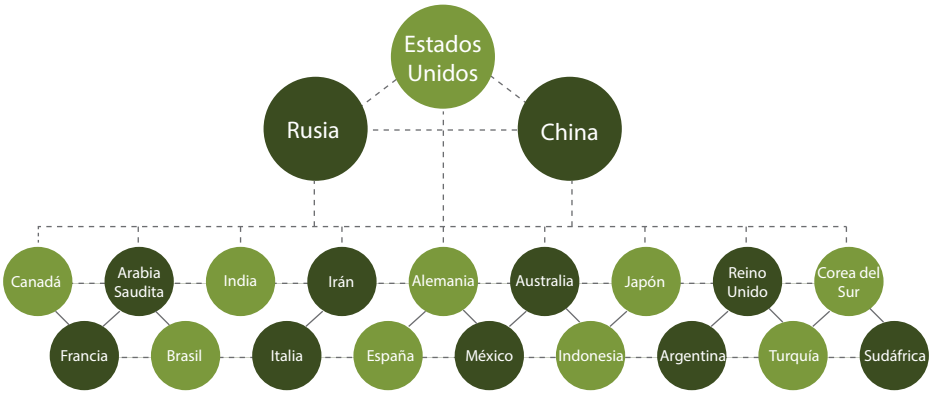
En el inicio de este capítulo se propuso hablar de los sucesos o los acontecimientos, como las guerras del siglo XIX, donde el orden mundial ha tenido cambios significativos, y por consiguiente, sobre la aparición de un sistema

multipolar, bipolar y unipolar con el transcurrir de las décadas (Barbe, 1987). A causa de los cambios en el sistema internacional, donde el equilibrio mundial es el fin para alcanzar la armonía entre los Estados, surge una nueva pregunta de relevancia: *¿cuál sería el sistema que brinde una mayor estabilidad en el contexto global? ¿Un sistema multipolar, uno bipolar o uno unipolar?*

En el mundo contemporáneo, los Estados han determinado como prioridad fortalecer sus capacidades en la búsqueda del liderazgo y emerger a un mayor protagonismo dentro de un escenario internacional. Es así como el Realismo estructural, o neorrealismo, es el pensamiento predominante de las RR. II., pese a la participación de actores no estatales en el sistema internacional (Hernández, 2008). Por lo anterior, el mundo continúa en una caracterización anárquica, donde se genera la posibilidad del surgimiento de nuevos actores internacionales desde la óptica de las amenazas a la seguridad.

Actualmente, la configuración del sistema internacional no solo se enfoca en los Estados. Por tanto, la globalización, la transnacionalización y la revolución informática han incorporado nuevos elementos, como la *estructura* y el *proceso*, donde la incorporación de nuevos aspectos, como el económico, el político, el social, el cultural y el militar, traspasa las fronteras, para definir una nueva configuración, donde no es solo uno o varios Estados, sino la incorporación de nuevos actores, en el sistema internacional (Orozco, 2014, p. 102). A pesar del ingreso de estos elementos, continúa la lucha por el dominio mundial, donde siempre existirá la preocupación por la alteración de alianzas que propicien el desequilibrio internacional (Orozco, 2014).

Figura 1. *Jerarquía de los 21 Estados principales del sistema internacional.*



Fuente: Orozco (2014).

A pesar de que actualmente la distribución del poder en el sistema internacional se encuentra en manos de tres potencias, que son Estados Unidos, China y Rusia, como lo muestra la figura 1, hay otros países emergentes que buscan tener un dominio regional. Como consecuencia, el mundo contemporáneo se enfoca en la multipolaridad, lo cual puede acarrear escenarios complejos que fortalezcan las amenazas para el sistema internacional, como lo identifica Nye (2002, citado por Orozco, 2014), cuando se refiere a "Estados soberanos contrarrestándose y rebotando unos contra otros como bolas de billar " (p. 109) en el ámbito de las RR. II. Esto resulta en un mundo complejo, donde hoy por hoy se dificulta hablar de hegemonía y dominio mundial, debido a las diferentes potencias que están luchando por alcanzar la supremacía, además de los organismos supranacionales, las empresas, los individuos poderosos y las organizaciones terroristas y criminales, entre otros.

Aspectos como la política, la sociedad, la religión, la aristocracia, la tecnología y la ciencia, los imperios, la academia, los militares y policías, así como lo económico, han tenido, a lo largo de la historia, diferentes posturas e intereses particulares a la hora de hablar sobre lo que es la guerra y, más aún, sobre cómo combatirla o no, por ser un negocio rentable para unos, o una necesidad de supervivencia, para otros. Los diferentes medios de comunicación se han convertido en una de las herramientas de mayor uso en los aspectos económico, político, social y militar, para satisfacer intereses por parte de actores estatales y no estatales, e incluso, como un pretexto para acciones bélicas (Pozo, 2010).

En conclusión, pese a la ambición de los Estados en cuanto a satisfacer sus intereses, existe la preocupación de ellos por mantener un equilibrio mundial evitando un escenario de caos, como la generación de una guerra similar a las que sucedieron a lo largo del siglo XX. El neorrealismo es el pensamiento de las relaciones internacionales que se aproxima al concepto de interés-Estado en el sistema internacional, dentro de un sistema anárquico, en el cual las amenazas reales y las potenciales requieren el uso de las FF. MM. para contrarrestarlas y defender los intereses de una nación (Álvarez, 2018).

Un problema para la seguridad, que se muestra de forma compleja y confusa

La seguridad, como concepto amplio, ha sido y será el eje central del desarrollo y la evolución de la humanidad y, sobre todo, la garante de la dignidad humana. En tal sentido, la seguridad y la supervivencia mantienen una estrecha relación en lo

que respecta a la libertad, la justicia y la paz de la Carta de las Naciones Unidas (OEA, 2003). Sin embargo, ¿son complementarias? Según Williams (2008), citado por Álvarez et al. (2018), "aunque la seguridad y la supervivencia a menudo estarían relacionadas, no son necesariamente sinónimos; mientras que la supervivencia sería una condición existencial, la seguridad implicaría la capacidad de perseguir ambiciones políticas y sociales requeridas" (p. 29). Esto permite ver una concepción más amplia de la seguridad, donde sus objetivos van más allá de la conservación en sí misma, pues también busca unos intereses en beneficio propio.

En ese orden de ideas, y tomando la seguridad como medio para anticipar, negar y contener las amenazas a la seguridad, el objetivo del presente apartado es caracterizar las amenazas a la seguridad multidimensional, a partir del enfoque y la doctrina planteados por la OEA y la ONU, teniendo como punto de partida la estructura y la filosofía de adopción de los términos en relación con las amenazas del documento de la Declaración sobre seguridad en las Américas, aprobado en octubre de 2003 por la OEA (2003), y el cual permitió evidenciar un enfoque novedoso para el momento, respecto a cómo llamar las amenazas y distinguirlas unas de otras, precisamente, por la cantidad de estas y por el impacto dentro del sistema internacional desde principios del siglo XXI, entre otras, por los ataques del 9-11, y que hasta el día de hoy continúan mutando; en especial, por su peligrosa relación con el ciberespacio.

Por lo anterior, se presentan los siguientes cuestionamientos: *¿qué amenazas se han consolidado en el sistema internacional? ¿Cuáles son las nuevas amenazas que afectan la seguridad de los Estados en común? ¿Las amenazas han mutado, y traspasan fronteras?* Dichos interrogantes han sido analizados por diferentes organizaciones y autores, lo cual permite explicación más minuciosa en el desarrollo de este apartado.

Actualmente, la preservación de los intereses en materia de seguridad es el tema prioritario de cualquier cumbre o cualquier reunión que se realice en el marco internacional. El concepto de seguridad fue delimitado por las Naciones Unidas en 1987 (Tello, 2000) como "una situación en la que los Estados consideran a resguardo de peligro para que se produzca un ataque militar, presión política o coerción económica, obteniendo con ello libertad de acción para continuar con su propio desarrollo y progreso" (p. 135). Eso indica la importancia que tiene el poder militar en la agenda de los Estados, por cuanto impacta los aspectos económico, político y social.

Con la caída del Muro de Berlín, la última década del siglo XX dejó al descubierto no solo el enquistamiento del comunismo en América Latina. También quedaron en evidencia las nuevas formas de afectación a la seguridad global que se habían configurado, incluso, años y décadas atrás. La preocupación por las guerras entre Estados —o peor aún, una guerra nuclear— fue por mucho tiempo el foco de atención de la seguridad, por lo que la inteligencia estratégica al servicio de los tomadores de decisiones no alcanzó a anticipar esta nueva forma de relacionamiento entre los seres humanos.

Resumiendo lo tratado por algunos autores que abordaron el tema de la guerra, como William Lind (2005), César Augusto Niño (2017) e incluso, los coroneles Qiao Liang y Wang Xiangsui, de la "Guerra Irrestricta" (1999) (citados por Álvarez, 2018), se llega al interrogante de si el mundo inició el siglo XXI inmerso en guerras de tercera, cuarta, quinta o sexta generación, o quizá, en una sin restricciones ni reglas o, tal vez, en una guerra totalmente híbrida, donde lo complicado es que, con seguridad, los humanos no se dieron cuenta. De hecho, las armas más modernas de quinta generación y la tecnología *stealth* ya circulan en el mundo, mientras algunos países viven en medio de guerras con armas artesanales.

De lo anterior, cabe suponer la posibilidad de que surja una guerra interestatal en cualquier parte del mundo, así como la posibilidad de que continúen los ataques terroristas, o de que las nuevas formas de criminalidad —como el narcotráfico, la trata de personas, el despojo de la tierra, la minería criminal, el tráfico ilegal de armas, el uso de armas de destrucción masiva o el reclutamiento forzado con diferentes fines— se fortalezca (Olaya et al. 2007). Esto permite evidenciar que el concepto simple de seguridad y defensa se ha quedado corto de sentido para dar respuesta a los problemas que han surgido desde entonces. Al respecto, la seguridad y defensa ha debido evolucionar a nuevos enfoques, como la seguridad internacional, la seguridad nacional, la seguridad cooperativa, la seguridad ciudadana, la defensa nacional y la defensa colectiva, entre otras tantas, sin dejar de mencionar la seguridad humana, la cual, a su vez, se enfoca en los miedos y los temores del ser humano.

Lo cierto es que todos esos sentidos dados a la seguridad y defensa buscan dar respuesta a las amenazas que proliferan en todo el planeta; en el caso del presente estudio, las que plantea la Declaración de las Américas de la Organización de Estados Americanos en el 2003 (OEA), al denominarlas como amenazas tradicionales y nuevas amenazas a la seguridad multidimensional, incluidas las vulnerabilidades sociales y ambientales. Y como se mencionó líneas

arriba, también se incluyeron otras fuentes documentales de la ONU y la OTAN de las cuales se extractaron otras amenazas.

Así las cosas, la definición que se da desde la multidimensionalidad a la seguridad tiene que ver con todo aquello que, además de las amenazas militares, impacta los aspectos económico, político y social, al traspasar fronteras y requerir la cooperación interagencial de los Estados, donde dicha cooperación se basa no solo se basa en el poder militar, sino que también abarca el uso de diferentes estrategias, como la diplomacia y la interacción de los actores estatales y no estatales (Font & Ortega, 2012). De igual modo, la OEA (2003) afirma que:

> Las amenazas, preocupaciones y otros desafíos a la seguridad en el hemisferio son de naturaleza diversa y alcance multidimensional y el concepto y los enfoques tradicionales deben ampliarse para abarcar amenazas nuevas y no tradicionales, que incluyen aspectos políticos, económicos, sociales, de salud y ambientales. (p. 3)

Conceptos como el de la seguridad nacional han sido ampliados, al cobijar ahora amenazas más allá de la tradicional guerra o el conflicto internacional; por tanto, dicho criterio de multidimensionalidad implica que las políticas de seguridad de los Estados deben incorporar e integrar todos los medios de la nación. Es claro, sin embargo, que, a pesar del surgimiento de estas nuevas amenazas, no se puede ignorar ni restar importancia a las amenazas tradicionales, que siguen siendo una preocupación en cuanto al equilibrio global, según la OEA. De acuerdo con Chinome Soto, dichas amenazas tradicionales "son aquellas en donde para su solución se hace necesario el empleo de la Fuerza Militar" (2017, p. 12), capacitada y entrenada para combatir los diferentes flagelos que generan afectación al Estado. Así las cosas, "las amenazas tradicionales a la seguridad y sus mecanismos para enfrentarlas siguen siendo importantes y pueden ser de naturaleza distinta a las nuevas amenazas, preocupaciones y otros desafíos a la seguridad y a los mecanismos de cooperación para hacerles frente" (OEA, 2003, p. 4).

La guerra, "tan antigua como el hombre mismo y […] arraigada en lo más profundo del corazón humano" (Keegan, 2014, p. 30), seguirá siendo "el más espectacular de los fenómenos sociales" (Bouthoul, 1971, p. 5), además de permanecer vigente en la vida de la especie humana, no obstante los grandes esfuerzos de muchos Estados y organismos supranacionales por detenerla, como parte de la diplomacia, y de la estrategia (Keegan, 2014) de supervivencia de todos en el planeta.

A pesar de que la seguridad permanece en la agenda de los Estados como garante para su desarrollo y su prosperidad, el surgimiento de la globalización a partir de la evolución tecnológica en la última década del siglo XX terminó por desaparecer el monopolio de la seguridad por parte de los Estados. Además, surgieron con mayor visibilización las manifestaciones sociales, políticas y culturales. Así, y tras el 9-11, los integrantes del Consejo de Seguridad se pusieron de acuerdo para combatir a escala global el terrorismo. Y en el hemisferio americano, Estados Unidos lideró una política de lucha contra dicha amenaza, de manera mayormente decidida. Una de esas respuestas es la propia Declaración de las Américas de 2003 (OEA). Por lo tanto, el compromiso, en el caso de la lucha contra el terrorismo debía ser de todos por igual. Incluso, el Consejo de Seguridad, sobre la base del derecho internacional, adelantó sanciones para quienes negociaran o patrocinaran cualquier tipo de actividad terrorista, lo cual se ha extendido a aquellos que, de la misma forma, lo hagan con países como Corea del Norte en su carrera nuclear, entre otros.

Es así, por tanto, cómo en la época contemporánea todos los poderes de la sociedad son afectados por la guerra y las nuevas amenazas. Y aunque ya se ha hablado de la guerra y el terrorismo, se hace necesario hablar de la otra nueva amenaza: el COT, definido como "una amenaza de naturaleza transnacional, flexible y opaca. Se trata de un fenómeno con una enorme capacidad desestabilizadora, que contribuye a debilitar el Estado y mina la buena gobernanza económica" (Gobierno de España, 2017, p. 62). En el COT se alberga una inmensa cantidad de amenazas, como el problema mundial de las drogas, el lavado de activos, la corrupción, la trata de personas, la minería ilegal, la falsificación de contrabando de medicamentos e insumos médicos y el reclutamiento forzoso, tan solo por mencionar unos pocos de la larga lista de amenazas relacionadas con el COT, por lo que se puede evidenciar la necesidad de una verdadera cooperación entre los Estados para contener tan gran problema del siglo XXI y evitar una mutación paralela a los males del planeta (Banegas, 2017).

Por lo anterior, el COT se suma a los retos de seguridad multidimensional, ya planteados, como el primer punto que debe encabezar las agendas de los Estados para minimizar las estrategias por parte de grupos terroristas, organizaciones criminales, e incluso, Estados criminalizados, entre otros. Lo cierto, a pesar de todo, es que en no todas partes del mundo se da la misma interpretación a lo aquí tratado.

Lo cierto es que las amenazas tradicionales y las nuevas amenazas que afectan actualmente a la humanidad son el resultado de una interminable lista

de causas. Es innegable que dichos males son parte de la cultura social histórica de la humanidad. A pesar de lo anterior, acabarlas en algún momento de la historia seguirá siendo una imperiosa necesidad. El problema para poder cumplir esta aspiración humana será si lo que le queda de historia a la especie es tiempo suficiente para lograrlo, y si, por lo tanto, la violencia entre congéneres seguirá siendo parte relacional de los seres humanos. Por lo tanto, "la guerra [y todas las amenazas a la seguridad en el siglo XXI son] un acto de violencia para obligar al contrario a hacer nuestra voluntad" (Clausewitz, 2005, p. 34), y por consiguiente, obtener poder, dominio y, principalmente, lucro.

En el mundo actual, eso es lo que busca un enemigo en el campo de combate, el cual, como escenario, se ha trasladado a las ciudades, a los parques naturales protegidos —como lo hace el narcotráfico en Colombia— y en general, a cualquier sitio. De hecho, ha llegado más allá de los dominios naturales, y ha alcanzado el ciberespacio. En suma, lo que persigue una organización criminal empeñada en imponer su negocio de narcotráfico en una nueva ruta usando la corrupción y los medios necesarios para lograrlo. Igualmente, un grupo terrorista que pretenda acabar con todo el mundo occidental, al considerarlo "pecador" por el solo hecho de pertenecer a otras religiones.

Por lo tanto, la complejidad de la proliferación de las amenazas a la seguridad plantea retos de anticipar, negar y contenerlas, ahora en el escenario ciberespacial, donde se potencializan las capacidades para hacer daño a la sociedad global. Cualquiera desde un computador puede buscar la forma de interferir en los planes de defensa de una nación, o la de robar información o dinero de corporaciones y bancos. Hasta negociar la vida de seres humanos. Finalmente, y para verlo desde una perspectiva más compleja, se plantean preguntas que en la realidad probablemente no tengan respuesta: ¿Quién es ese cualquiera que está al otro lado de un computador? ¿Dónde estará? ¿Cómo combatirlo? ¿Pueden hacerlo el poder y la capacidad militar de un Estado?

Las amenazas tradicionales y las nuevas amenazas de la seguridad multidimensional

El objetivo del presente apartado está enfocado en caracterizar las amenazas de la seguridad multidimensional, a partir de lo planteado por la OEA, integrando otras amenazas encontradas en la ONU y la OTAN. Para llevar a cabo dicha caracterización, es necesario entender que la seguridad y defensa de los Estados

mantiene una constante evolución y genera nuevas estrategias cooperativas desde los organismos supranacionales buscando negar, contener y anticipar los efectos que producen las amenazas. Después de la Guerra Fría, es más claro el panorama de seguridad global, puesto que las nuevas amenazas se dejaron ver con mayor claridad.

Una *amenaza*, según Banegas, es entendida como la acción premeditada por parte un adversario que tiene la capacidad de causar daño (2017). Del mismo modo, los Descriptores de la Salud la definen como:

> La probabilidad de que un fenómeno, de origen natural o humano, se produzca en un determinado tiempo y espacio. Peligro (potencial) de que las vidas o los bienes materiales humanos sufran un perjuicio o daño. Posibilidad a la que están expuestos los pobladores de un determinado lugar. (Biblioteca Virtual en Salud-DeCS, 2022)

La evolución de las amenazas, en lo que se refiere a su concepto, fines que persigue el terrorismo o la criminalidad al afectar el desarrollo y la dignidad humana por medio de la materialización de amenazas y modo de llevarlas a cabo, conlleva a la amenaza en el mundo contemporáneo, es decir, a la "hibridación" (Bartolomé, 2019) de todas las formas de violencia, precisamente, por la complejidad que esto trae para la seguridad. En palabras del Teniente General James N. Mattis, y del Teniente Coronel Frank Hoffman (Ret.), del Cuerpo de Marines de los Estados Unidos (en inglés, USMCR, por las iniciales de United States Marine Corps).

> No nos enfrentamos tanto a una serie de cuatro desafíos separados como a la combinación de enfoques novedosos, una fusión de diferentes modos y medios de guerra [:] terrorismo, insurgencia, guerra sin restricciones, guerra de guerrillas o coerción por parte de narcodelincuentes. (Matis & Hoffman, 2005, p. 1) [traducción propia]

Sin embargo, y para hacer claridad sobre lo que es la "amenaza híbrida", el glosario de terminología de uso conjunto del Estado Mayor de la Defensa de España (2019) la define como:

> Aquella que emplea de forma adaptativa todo tipo de instrumentos de poder; procedimientos convencionales junto a tácticas irregulares y a actividades terroristas; crimen organizado; nuevas tecnologías; ataques en el ciberespacio; presión política y múltiples tipos de herramientas de información y desinformación, incluyendo las noticias falsas y la mentira en sí misma. (p. 7)

Lo anterior, y sin salir de la línea ideológica de lo tratado hasta ahora, solo evidencia, particularmente, asuntos con un alto grado de similitud, pues Mattis y Hoffman particularizan su enfoque desde la perspectiva de seguridad de Estados Unidos.

Así las cosas, y prosiguiendo con la discusión propia de caracterizar las amenazas, de acuerdo con lo planteado, en la tabla 2 se presentan algunas amenazas desde la perspectiva de la Junta Interamericana de Defensa (citada en Chinome, 2017), como organismo parte de la OEA, y el cual se refiere a la clasificación de las amenazas.

Tabla 2. *Clasificación de las amenazas, según la Junta Interamericana de Defensa*

Tradicionales	No tradicionales	Estructurales
Proliferación de armas de destrucción masiva (AADM)	Terrorismo	Pobreza
	Tráfico de drogas ilícitas, narcoterrorismo y delitos conexos.	Degradación del medio ambiente.
	COT.	Corrupción.
Problemas limítrofes históricos pendientes	Problemas tribales, étnicos y políticos internos.	Migración masiva y descontrolada.
	Catástrofes naturales.	Violencia ciudadana.
	Transporte y depósito de desechos nucleares o radioactivos.	VIH/Sida y enfermedades o epidemias.
Lucha por recursos vitales	Tráfico ilícito de armas.	Diferencia tecnológica.
	Crimen cibernético.	Márgenes importantes de desempleo.
Lucha antiguerrilla y contrainsurgencia	Lavado de dinero.	Crisis económicas.
	Tráfico de personas.	

Fuente: Junta Interamericana de Defensa, *Conceptualización de los nuevos desafíos y amenazas a la seguridad hemisférica* (2003), citada por Chinome (2017) .

Por lo anterior, se aclara que la existencia, la mutación y la aparición de nuevas amenazas han obligado a hacer un nuevo planteamiento respecto al alcance de la seguridad y defensa nacional de los Estados. Lo anterior, debido a que tales amenazas obligan a enfrentarlas con nuevos retos cooperativos, a partir de los organismos supranacionales, para que trabajen de manera coordinada.

Fuentes documentales para la caracterización de las amenazas

Por todo lo planteado, a continuación se presenta en detalle la caracterización desarrollada a partir del objetivo del presente apartado. Lo anterior se hizo inicialmente a través de la observación de los tres principales organismos previstos desde el inicio: la ONU, la OEA y la OTAN, y dentro de la ONU, específicamente, la Asamblea Genera (ONU-AG) y la Organización de Naciones Unidas contra la Droga y el Delito (UNODC), como se muestra a continuación:

- Carta de las Naciones Unidas (2003)
- Tratado del Atlántico Norte (1949)
- Declaración sobre Seguridad en las Américas (2003)
- Amenazas transnacionales. Hacia un mundo justo, seguro y pacífico regido por el Estado de derecho (Organización de Naciones Unidas [ONU], 2021a)

Por lo anterior, y de acuerdo con el análisis de los documentos ya relacionados, seguidamente se evidencian la contextualización de las amenazas tradicionales y las nuevas amenazas a la seguridad.

Amenazas tradicionales

Como ya se ha argumentado, y en concordancia con el concepto de amenazas tradicionales de la OEA, ha sido la guerra la amenaza que, desde lo que conoce la historia, ha acompañado al ser humano en el leguaje de la violencia. Además, y con la aparición de los Estados nación, y sin dejar de lado su sentido histórico, podría decirse que ha evolucionado hasta el punto de que cabe afirmar que "la principal amenaza a la seguridad internacional provenía de agresiones externas por parte de otros Estados, que generalmente eran de carácter militar" (Olaya et al., 2007, p. 4).

En este sentido, en la tabla 3 se plantea la amenaza tradicional de la guerra, a partir de las acepciones presentadas por los organismos allí descritos, y los cuales emplean los términos *amenazas al territorio* y *conflictos entre Estados* para hacer, quizá, una interpretación menos fuerte y menos compleja del término *guerra*. Sin embargo, seguirá siendo lo mismo.

Tabla 3. *Clasificación de las amenazas tradicionales*

Amenazas tradicionales	ONU (1945)	OTAN (1949)	OEA (2003)	ONU-AG (2004)
Amenazas al territorio nacional.	X	X	X	X
Conflictos entre Estados.				

Fuente: elaboración propia.
Nota: datos tomados de la ONU (1945), la OTAN (1949), la OEA (2003) y la ONU-AG (2004).

Nuevas amenazas

Por otra parte, en la tabla 4 se reportan 24 nuevas amenazas. Cabe observar que son pocas las amenazas mencionadas en todos los documentos. El terrorismo, así como el acceso, la posesión y el uso de armas de destrucción en masa, la DOT, el problema mundial de las drogas, el lavado de activos y la corrupción son los más mencionados, sin que ello reste importancia ni disminuya la preocupación respecto a las otras amenazas mencionadas.

Tabla 4. *Clasificación de las nuevas amenazas*

	Nuevas amenazas	OEA (2003)	ONU-AG (2004)	OEA (2020)	UNODC (2021)
1	Terrorismo.	X	X	X	X
2	Acceso, posesión y uso de armas de destrucción masiva.	X	X	X	X
3	DOT.	X	X	X	X
4	Problema mundial de las drogas.	X	X	X	X
5	Lavado de activos.	X	X	X	X
6	Tráfico ilícito de armas de fuego.	X	X	X	X
7	Trata de personas.	X	X	X	X

	Nuevas amenazas	OEA (2003)	ONU-AG (2004)	OEA (2020)	UNODC (2021)
8	Corrupción.	X	X	X	X
9	Ataques a la seguridad cibernética.	X		X	
10	Minería ilegal.			X	
11	Reclutamiento forzoso.			X	
12	Falsificación de contrabando de medicamentos y de insumos médicos.			X	X
13	Uso indiscriminado de minas antipersonales.			X	
14	Extorsión.			X	
15	Delincuencia marítima.				X
16	Ataques a la infraestructura económica y vial.			X	
17	Tráfico ilícito de migrantes.			X	X
18	Pobreza extrema.		X		
19	VIH/Sida y otras enfermedades.		X		
20	Degradación del medio ambiente.		X		
21	Prevención del delito y justicia penal (discriminación de género).		X		
22	Delitos contra la vida silvestre y los bosques.		X		
23	Violencia doméstica.			X	
24	Trabajo infantil.			X	

Fuente: elaboración propia (2021).

Nota: datos tomados de la OEA (2003), la ONU-AG (2004), la OEA (2020) y UNODC (2021).

Como se puede observar desde la cantidad de amenazas presentadas, ya hay un impacto generado en el mundo contemporáneo. A dichas amenazas no son ajenas ni tan siquiera las grandes potencias; de ahí el compromiso planteado desde lo supranacional. Bien pueden existir algunas amenazas capaces de generar un mayor daño que otras o, peor aún, se conviertan en herramientas de grupos delincuenciales para obtener recursos financieros que sostienen dichas actividades delictivas. Pero incluso más compleja es su fusión con el ciberespacio. De ahí las nuevas acepciones de cibercrimen, ciberdelito, ciberterrorismo y ciberguerra, entre otras.

Por otra parte, del análisis anterior se podría llegar a otro, más esclarecedor, dentro de las mismas nuevas amenazas. Para ello, se consideraron los siguientes criterios: las amenazas de mayor impacto en el marco de la OEA y la ONU desde 2003 hasta 2021 fueron 24; sin embargo, al hacer la matriz documental de los cuatro documentos mencionados, se extrajeron once amenazas que se tipifican como las de mayor relevancia en cada documento.

Finalmente, en la tabla 5 se agrupan las amenazas de mayor preponderancia, de acuerdo con los documentos relacionados en la tabla 4; es decir, los criterios que condujeron a presentar el orden en 3 grupos en la tabla 5.

Tabla 5. *Clasificación nuevas amenazas*

<table>
<tr><th>I GRUPO</th><th>II GRUPO</th><th>III GRUPO</th></tr>
<tr><td>Terrorismo</td><td>Problema mundial de las drogas.</td><td>Ataques a la seguridad cibernética.</td></tr>
<tr><td rowspan="2">Acceso, posesión y uso de armas de destrucción masiva.</td><td>Lavado de activos.</td><td rowspan="2">Falsificación de contrabando de medicamentos e insumos médicos.</td></tr>
<tr><td>Tráfico ilícito de armas de fuego.</td></tr>
<tr><td rowspan="2">DOT.</td><td>Trata de personas.</td><td rowspan="2">Tráfico ilícito de migrantes.</td></tr>
<tr><td>Corrupción.</td></tr>
</table>

Fuente: elaboración propia (2021).
Nota: datos tomados de la OEA (2003), la ONU-AG (2004), la OEA (2020) y la UNODC (2021).

Como cabe deducir, en la tabla 4 se enmarcan con mayor énfasis las nuevas amenazas en el mundo contemporáneo: el terrorismo, los ataques a la seguridad cibernética, la DOT o el acceso y la posesión de armas de destrucción masiva (OEA, 2003), todas las cuales actúan de manera transversal en ecosistemas criminales (Álvarez Calderón & Rodríguez Beltrán, 2018). Esto quiere decir que la evolución de las nuevas amenazas en un mundo globalizado permite a grupos criminales interactuar en un entorno multifacético, donde amenazan la estabilidad internacional en los aspectos económico, político y social (Álvarez & Rodríguez, 2018).

Nuevas amenazas desde la perspectiva regional

Partiendo de la transnacionalidad de las amenazas —tanto las que se conocen y se padecen en el hemisferio como las que se viven en otras partes del planeta—, todas ellas pueden relacionarse en cualquier momento y en cualquier lugar. Lo cierto es que en todas partes los mecanismos de protección para contrarrestarlas podrían no ser lo suficientemente efectivos para minimizar el riesgo; en especial, en el subcontinente latinoamericano, donde la defensa ante estas nuevas amenazas se enfoca en el poder militar (Blackwell, 2015). De la misma forma, en el contexto regional, según Banegas (2017), la percepción de amenazas priorizadas por subregión (Mercosur, Países Andinos, Centroamérica y el Caribe) tiende a poner como prioridad en las agendas de seguridad el terrorismo, el narcotráfico y el crimen organizado, según publica la Academia Nacional de Estudios Políticos y Estratégicos (Anepe) (Banegas, 2017), y como se muestra en la tabla 6.

Lo anterior, por otra parte, guarda relación directa con las amenazas mencionadas en todos los documentos ya relacionados, y no sin algunas diferencias, además de sumar amenazas como las que acechan al medio ambiente en el Caribe, o la pobreza y las carencias sociales en Centroamérica, y respecto a las cuales, desde la definición de amenaza y la consideración política de llamarlas así, hay total autonomía, a pesar de que en la Declaración de las Américas se hable de una vulnerabilidad social y ambiental, que, sin embargo —y de acuerdo, también, con las circunstancias en que se presenten— pueden desembocar en una amenaza.

Tabla 6. *Percepción de amenazas priorizadas por subregión*

Mercosur	Países andinos	Centroamérica	Caribe
Narcotráfico.	Narcotráfico.	Narcotráfico.	Narcotráfico.
Terrorismo.	Terrorismo.	Terrorismo.	Terrorismo.
Tráfico de armas.	Pobreza y carencias sociales.	Medio ambiente y desastres naturales.	Pobreza y carencias sociales.
Crimen organizado.	Guerrillas y grupos subversivos.	Crimen organizado.	Medio ambiente y desastres naturales.
Medio ambiente y desastres naturales.	Tráfico de armas.	Pobreza y carencias sociales.	Tráfico de armas.
Pobreza y carencias sociales.	Crimen organizado.	Tráfico de armas.	Crimen organizado
Guerrillas y grupos subversivos	Medio ambiente y desastres naturales.	Guerrillas y grupos subversivos.	

Fuente: F. Rojas Aravena, en Alfaro Banegas: Estrategias para combatir las amenazas multidimensionales en la región, Banegas, 2017.
Nota: datos tomados de la ONU (1945), la OTAN (1949), la OEA (2003; 2020), la ONU-AG (2004) y la UNODC (2021).

En conclusión, caracterizar las amenazas en materia de la seguridad multidimensional a partir de lo planteado por la OEA y la ONU, la UNODC y la OTAN permite un mejor acercamiento a las amenazas que están afectando el mundo contemporáneo para proponer los posibles retos que pueden darse a lo largo de las próximas décadas del siglo XXI, lo cual se argumenta en la parte final del presente escrito.

Este hallazgo permite no solo presentar un resultado de investigación: debe, además, llevar a nuevas conclusiones sobre el rumbo de la seguridad en el planeta, así como la solidaridad cooperativa entre Estados y organismos supranacionales. Enfoques desde África, Europa o Asia, por su parte, dejarán una mayor impresión de la vulnerabilidad humana como consecuencia de la proliferación de las *amenazas a la seguridad*, en todo el sentido de dicho término.

Retos y desafíos en materia de seguridad en las próximas décadas del siglo XXI

En este último apartado, y habiendo presentado las amenazas tradicionales y las nuevas amenazas a la seguridad, el objetivo es plantear los posibles retos del mundo, en el marco de la seguridad para las próximas décadas de la presente centuria. Si bien es cierto que no se puede tener la certeza sobre lo que va a suceder en próximos decenios, es preciso señalar que el futuro tendrá escenarios aún más complejos que los que vive la humanidad actual, a causa del desarrollo desmesurado de la tecnología, principalmente, y por el aceleracionismo que ello le imprime a la vida diaria del planeta. En este sentido, se visibilizaron once retos a lo largo del presente capítulo, que se presentan en la tabla 7, y seguidamente se procede a su descripción.

Tabla 7. *Retos y desafíos en materia de seguridad en las próximas décadas del siglo XXI*

1	Tendencias desde el enfoque del secretario general de las Naciones Unidas.
2	Búsqueda de una seguridad inteligente.
3	Retos y desafíos en el relacionamiento humano en el siglo XXI, a partir de la colectividad y del cooperativismo.
4	Administrar el desarrollo tecnológico en beneficio de la seguridad.
5	El dominio de la información.
6	Contener la guerra y el terrorismo como problemas de seguridad nacional.
7	Control de las armas de destrucción masiva.
8	El problema de las pandemias, y su repercusión respecto a la criminalidad y el terrorismo.
9	El ciberterrorismo.
10	El control del desarrollo de la tecnología para mejorar y no afectar la vida humana.
11	El aumento demográfico mundial y las consecuencias en el cambio climático.

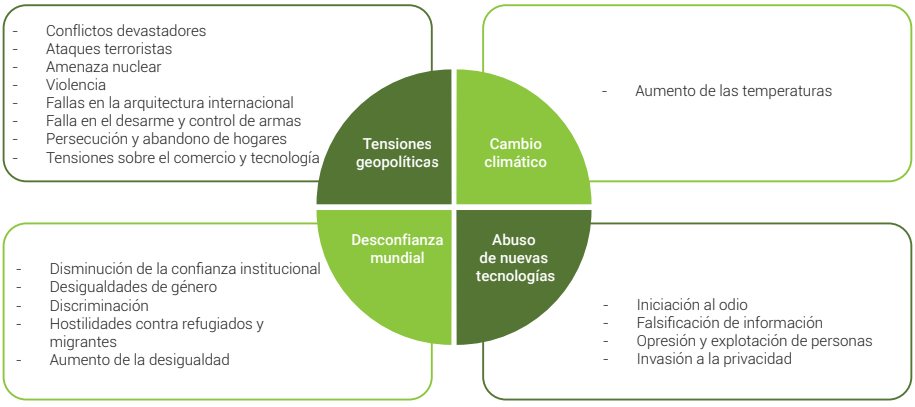
Fuente: elaboración propia.

Tendencias desde el enfoque del secretario general de las Naciones Unidas

De acuerdo con una de las recientes intervenciones de António Guterres, Secretario General de Naciones Unidas (2020), en lo referente al orden internacional que vive el planeta, es posible coincidir con lo que él denomina "los cuatro Jinetes del Apocalipsis", y que hoy por hoy afectan el progreso del mundo: tensiones políticas, cambio climático, desconfianza mundial y abuso de nuevas tecnologías, y que para este análisis se interpretarán como tendencias.

En la figura 2 se presenta un resumen de lo planteado por Guterres, y que guarda relación con el diagnóstico de las amenazas a la seguridad presentadas en el apartado anterior, y donde se da cuenta de la complejidad que debe manejar el planeta entero, y de los retos que debe enfrentar en el corto plazo, de cara a o que depara el siglo XXI. No obstante, es necesario tener en cuenta todas y cada una de las afectaciones propias de la pandemia del COVID-19 y las que podrían generarse a consecuencia esta, que, además, afecta por igual al mundo entero.

Figura 2. *Diagnóstico de amenazas a la seguridad*



Fuente: Elaboración propia con datos de OEA (2003) y Naciones Unidas (2020).
Nota: enfoque del secretario general de las Naciones Unidas, en el que generaliza sobre las cuatro tendencias que afectan al desarrollo del planeta.

En tal sentido, los "cuatro jinetes de apocalipsis", o tendencias —como ya se las llamó en este trabajo, para darle un enfoque mayormente académico—, y desde el lenguaje de la seguridad multidimensional desarrollado en la presente investigación, Guterres plantea, en cada una, algunas de las amenazas

ya caracterizadas en el apartado anterior, y otras, que, desde la perspectiva del secretario general de las Naciones Unidas, incluye desde su punto de vista global.

Se espera, con este enfoque analítico a partir de Guterres, dar mayor fuerza a la parte concluyente que se planteó al final del resultado de la caracterización de las amenazas.

Búsqueda de una seguridad inteligente

Para entender cómo focalizar la atención en lo planteado, sin descuidar algún tipo de amenaza emergente, Adam Blackwell (2011), quien fue secretario de Seguridad Multidimensional en la OEA, y luego, presidente del Consejo para la Agenda Global del Tráfico Ilícito y Crimen Organizado para el Foro Económico Mundial, planteó en el Discurso de Surinam la importancia de identificar "las necesidades a satisfacer y de los vacíos a superar en materia de seguridad", mediante la búsqueda de una "seguridad inteligente" (2011) que contribuya a orientar esfuerzos comunes y enfrentar los retos en materia de seguridad.

Este concepto implica la integración en todas las actividades humanas a partir de los siguientes criterios:

- Una identificación objetiva y basada en evidencia de los temas que serán objeto de la acción.
- Propuestas basadas en necesidades y capacidades nacionales o regionales, con el objeto de garantizar el apropiamiento por parte de los beneficiarios de los proyectos y su sustentabilidad.
- Propuestas basadas en experiencias positivas, y en alianza con actores relevantes.
- Un enfoque multidimensional que asegure una respuesta sistémica a los problemas.
- Evaluación de los resultados.

Retos y desafíos en el relacionamiento humano en el siglo XXI, a partir de la colectividad y del cooperativismo

Es importante recalcar que finalizando la centuria anterior y a principios del siglo XXI, aparecieron nuevos retos, en un mundo donde los conflictos entre los Estados se redujeron significativamente; y aunque su amenaza sigue vigente, el surgir de nuevos desafíos a la seguridad, como lo menciona Jiménez (2019), generó nuevas formas de relacionamiento humano desde la "violencia, militarismo,

armas nucleares, conflicto global, cooperación, derechos humanos, represión, sexismo, movimientos globales y cambio social, además, seguridad común, justicia económica, conflictos étnicos, proliferación nuclear, conversión nuclear, violencia cultural y simbólica, Norte-Sur y Sur-Sur, género-militarismo-desarrollo" (p. 123).

Esto conlleva hoy, más que nunca, que se integren los Estados con la participación de las organizaciones internacionales, teniendo el objetivo común de evitar que dichas amenazas incrementen la posibilidad de generar daños a la seguridad global antes de que sea demasiado tarde para controlarlas. Lo anterior, entre otras, a través de seguridad colectiva y cooperativa, pero no sectorizada por regiones, como sucede con la OTAN: por el contrario, una seguridad de carácter global, cobijando a todos por igual, en beneficio, fundamentalmente, de la supervivencia humana.

Administrar el desarrollo tecnológico en beneficio de la seguridad

Si se hace un análisis retrospectivo, se evidencia que las amenazas a finales del siglo XX se enmarcaban en un entorno que las hacían predecibles, controlables y detectables. Sin embargo, con los avances tecnológicos del siglo XXI, el aumento de la multipolaridad y la dispersión del poder, las nuevas amenazas afianzan su capacidad destructiva en la globalización y en las bondades del ciberespacio, el cual será un escenario de mayor alcance, donde las fronteras físicas no serán un impedimento para los nuevos actores.

De igual manera, las nuevas amenazas que se desarrollen en este entorno ciberespacial serán difíciles de controlar y de mitigar. Al respecto, según el Instituto Español de Estudios Estratégicos (2010), "el ciberespacio será el nuevo campo de batalla, debido a los riesgos y amenazas que su uso masivo plantea" (p. 30), por lo que la administración de la tecnología y el alcance ciberespacial deberán ser regulados y controlados para buscar, de alguna manera, que no sean explotados por la maldad.

Asimismo, el mundo de la información generará conmoción en las relaciones sociales, donde puede surgir el interrogante de si en las próximas décadas habrá un mejor entendimiento y un mejor fortalecimiento de las relaciones humanas, que permitan afianzar las coaliciones entre los Estados para mitigar amenazas en un ambiente ciberespacial.

El dominio de la información

Wallerstein (citado por Jiménez, 2019) menciona que "los 'próximos 25-50 años serán unos años terribles en términos de las relaciones sociales' y que, del mismo modo, '[…] serán unos años excepcionales en el mundo del conocimiento ya que la crisis sistémica forzará a la reflexión social'". Por ende, en las futuras décadas el dominio de la información será un punto decisivo para mantener la paz global, o podrá ser el detonante de un conflicto de Estados.

Contener la guerra y el terrorismo como problema de seguridad nacional

Una de las amenazas tradicionales analizadas en el presente documento fue el conflicto entre los Estados; de igual forma, se mencionaron varias apreciaciones que algunos autores propusieron dentro de un estudio exhaustivo del concepto de la guerra. Por otra parte, si se agrega a lo anterior el terrorismo, es posible identificar una mayor participación de organizaciones terroristas como el Estado Islámico (EIIL), Al-Qaeda y Boko Haram, las cuales usan la violencia para desequilibrar los órganos supranacionales (OIET, 2020), lo que genera una confluencia y una cercanía complejas entre los conflictos armados y el terrorismo, debido, entre otras, a una mayor articulación, lo que genera caos y nuevas formas de atacar a los entes gubernamentales.

En la actualidad, el terrorismo, por ser uno de los mayores retos del siglo XXI, se convierte en el talón de Aquiles de las estrategias de seguridad de las grandes potencias desde el inicio del siglo (OIET, 2021). Al respecto, la ONU (2018), afirma que "el terrorismo ha pasado a ser uno de los problemas más graves de nuestra época y ningún país está a salvo de su amenaza ni puede hacerle frente por sí solo" (p. 1). La amenaza terrorista en cualquier parte del mundo produce el desequilibrio necesario para afectar los derechos básicos del ser humano. Y de igual manera, impacta negativamente el desarrollo económico y social de los Estados, lo cual lo hace uno de los retos trascendentales del futuro (ONU, 2021a).

Control de las armas de destrucción masiva

Simultáneamente con lo anterior, existe una gran preocupación en lo referente a la falta de control a las armas de destrucción masiva (ADM), la cual se acrecienta cada día más. Es así como la mayoría de los países que cuentan con la tecnología y los recursos para construirlas, buscan tratados como "La no Proliferación

de las Armas Nucleares (TPN)" para mantener el equilibrio mundial (ONU, 2021a, p. 16). Sin embargo, no todos los países adoptan las resoluciones supranacionales, como es el caso de Corea del Norte y, posiblemente, Irán, en los cuales se mantiene una perenne desconfianza. De igual forma, algunos grupos terroristas contemplan estrategias respecto al uso de armas no convencionales, como la potencial amenaza del terrorismo químico, que es otra manera de causar daño irreversible a la especie humana.

Frente a lo anterior, según el Anuario del Terrorismo Yihadista 2020, Al Qaeda tratará de exportar fórmulas químicas a Europa, o militantes de Daesh intentarán fabricar un artefacto químico improvisado en suelo australiano, todo lo cual representa un gran desafío en el panorama internacional de la actualidad, en términos de seguridad interna y salud pública (OIET, 2020, p. 133). Esto permite evidenciar un inminente riesgo a la seguridad global, internacional y multidimensional en las próximas décadas, al haber una simbiosis de terrorismo con armas de destrucción masiva, sumado ello a la amenaza de un posible conflicto de Estados; todo lo anterior, financiado desde el narcotráfico, el tráfico de armas y la minería criminal, entre una variedad de amenazas que componen el COT, fortalecido, por otro lado, por la corrupción.

El problema de las pandemias y su repercusión respecto a la criminalidad y el terrorismo

Actualmente, las organizaciones internacionales abordan las preocupaciones que están afectando a los Estados. Es así como en el documento *Resolución promoción de la seguridad hemisférica: un enfoque multidimensional*, la OEA menciona la situación actual de la pandemia del COVID-19, y destaca su afectación directa al sistema global, y enfatiza amenazas como la DOT y otras actividades ilícitas, las cuales impactan la seguridad hemisférica (OEA, 2020, p. 3). Por consiguiente, la lucha contra la delincuencia se convierte en un desafío para los Estados, y eso requiere proponer estrategias de seguridad que afiancen la seguridad cooperativa y busquen un desarrollo sostenible para la próxima década.

La DOT abarca múltiples amenazas, como se muestra en la tabla 4, y las cuales son viables por el costo-beneficio para los grupos terroristas, debido al alto impacto mediático en el sistema internacional. Es así como la simbiosis de las nuevas amenazas trabaja de manera mancomunada para generar daños en los aspectos económico, político y social de los Estados. Según el Council of the European Union, General Secretariat of the Council (2009), el tráfico

transfronterizo de drogas, mujeres, inmigrantes ilegales y armas representa una parte importante de las actividades de las bandas de delincuentes, puede tener vinculaciones con el terrorismo (p. 32). Esto permite visualizar las tendencias de las nuevas amenazas y la dinámica del entorno en que se desenvuelven, lo cual, sumado a la tecnología, se convierte en un peligro latente para la seguridad global.

El ciberterrorismo

En la última década, el ambiente cibernético ha comenzado a ser el centro de atención para los Estados, por los ataques que han sufrido diferentes naciones. Según Cymerman (citado por el Instituto Español de Estudios Estratégicos, 2010), "Irán sufrió el 27 de septiembre de 2010, de confirmarse, el ataque cibernético más grande de la historia. Los sistemas de control de la central nuclear de Bushehr, así como de otras industrias, se vieron afectados por un virus de una potencia sin precedentes, denominado Stuxnet" (p. 16), de manera que esta amenaza, la cual se considera ciberterrorismo, se proyecta como uno de los principales retos respecto a las estrategias de seguridad mundial.

El ciberterrorismo es una amenaza sigilosa, lo cual incrementa su peligrosidad; es como entrar a un sótano oscuro con múltiples peligros, sin poder observarlos, lo que puede ocasionar un accidente de consecuencias fatales. Hoy en día se depende sobremanera del manejo de la información a través de la web; es más, el aspecto económico moderno se maneja a través de ese medio, donde la infraestructura, el comercio y la distribución de energía requieren al mundo cibernético para ser competitivos (Council of the European Union, General Secretariat of the Council, 2009). Además, según el Instituto Español de Estudios Estratégicos (2010), "el ciberespacio ha experimentado un enorme y veloz desarrollo, así como la dependencia que nuestra sociedad tiene de él, lo que contrasta con el menor y lento avance en materias de ciberseguridad" (p. 52). En otras palabras, el entorno que actualmente se está manejando espera mayor participación de otros actores, y requiere, por tanto, que la seguridad establezca mecanismos para mitigar los avances propios del flagelo del ciberterrorismo, y así evitar un colapso del equilibrio global.

El control del desarrollo de la tecnología para mejorar y no afectar la vida humana

El ser humano se ha caracterizado por su ingenio para construir y diseñar elementos o herramientas para su supervivencia. Hoy por hoy, la tecnología le ha permitido mejorar su calidad de vida en varios aspectos. No obstante, a la tecnología se la puede considerar un arma de doble filo, que puede llevar a un desenlace más peligroso que lo que aparenta ser. Lo anterior podría ser visto como exagerado, pero si se observan con detenimiento las publicaciones de organizaciones internacionales, tal vez la humanidad no se encuentre lejos de tan negativa realidad.

De acuerdo con el documento *Actividades del sistema de las Naciones Unidas para la aplicación de la Estrategia Global de las Naciones Unidas contra el Terrorismo*, la inteligencia artificial, la robótica, la biotecnología e internet (Asamblea General, 2018) han generado avances importantes para la humanidad en cuanto a conectividad y desarrollo sostenible. Sin embargo, según:

> Es probable que los terroristas mejoren su capacidad ofensiva para aprovechar la creciente interconexión de ciertos sectores, como la banca y las finanzas, las telecomunicaciones, los servicios de emergencia, el transporte aéreo, marítimo y ferroviario, y el suministro de energía y agua, a fin de llevar a cabo ciberataques contra esas infraestructuras vitales. (Asamblea General, 2018, p. 4)

Por esa razón, se requiere la cooperación entre los Estados para edificar barreras de protección en materia de ciberseguridad e inteligencia artificial, pues una amenaza que actúe en el ciberespacio es compleja de atacar si no se cambia la forma de pensar, o si no se innova para mitigar el riesgo derivado del terrorismo o de la DOT.

El aumento demográfico mundial y las consecuencias en el cambio climático

La demografía es un aspecto importante para tener en cuenta, según la ONU (citada por Olabe & González, 2008), "la actual población de 6.600 millones de personas seguirá creciendo hasta alcanzar en 2050 los 9.000 millones" (p. 176). Esto acarrea consecuencias como un mayor consumo de energía, lo cual, a su vez, requiere la explotación de recursos no renovables, como el petróleo, el gas y el carbón (Olabe & González, 2008). Adicionalmente, el hecho de buscar productividad para el sostenimiento de la población ha ocasionado impactos negativos

para el medio ambiente. Por ejemplo, la ONU ha argumentado que el cambio climático "es el mayor desafío de nuestro tiempo y del futuro" (ONU, 2021b).

El cambio climático es un "problema de seguridad", de acuerdo con el consejo de seguridad de la ONU realizado Inglaterra en 2007 (Olabe & González, 2008). Este problema de grandes magnitudes puede desencadenar peligros para la humanidad como el calentamiento global, que se ha visto en incremento por las actividades humanas en cuanto a industrialización. Según el informe de *Calentamiento global de 1,5 grados centígrados*, del Grupo Intergubernamental de Expertos sobre el Cambio Climático (en inglés, IPCC, por las iniciales de Intergovernmental Panel on Climate Change), se "prevé un aumento de 1,5 grados centígrados entre el 2032 y el 2050" (IPCC, 2019). Tal situación eleva los riesgos en salud mundial, como la escasez del agua y alimentos, y ello afecta todos los ámbitos de la seguridad, debido a que potencializa amenazas multidimensionales como el terrorismo, la delincuencia o el crimen transnacional, o la posesión y el uso de armas de destrucción masiva, las cuales han evolucionado tecnológicamente y se desenvuelven en un ambiente cibernético.

Otros retos, que vinculan lo anterior, los presentó, en una entrevista, Yuval Noah Harari, quien afirma que "la energía nuclear, cambio climático y la disrupción tecnológica" son los desafíos que tendrá el ser humano para la supervivencia (Harari, 2018). Esto demuestra la importancia del uso adecuado de la tecnología, sector en el que los avances han sido sustanciales con el transcurrir de los años; sin embargo, una de las mayores amenazas que están impactando el mundo contemporáneo, y que está ya siendo empleada por grupos delincuenciales, es la disrupción tecnológica, la cual tendrá impacto en la gestión de la seguridad integral (Álvarez & Ramírez, 2020; Guillén, 2020).

Finalmente, y en análisis comparativo con el reporte de riesgos globales y la evaluación de amenazas de la comunidad de inteligencia de Estados Unidos de 2022, lleva a coincidir con los desafíos que argumentan los autores ya mencionados, donde los riesgos de mayor impacto a mediano y largo plazo de la próxima centuria son las armas de destrucción masiva, los avances tecnológicos adversos, la crisis de recursos naturales y las fallas en el control del cambio climático (McLennan & Grupo, 2021; Office of the Director of National Intelligence, 2021).

Por tanto, la tecnología será el punto de inflexión que permitirá a la humanidad evolucionar hacia nuevas estrategias en los aspectos económico, político y social, en un escenario donde no será fácil adaptarse a nuevos escenarios complejos; especialmente, en materia de seguridad, y cuando el uso de la inteligencia

artificial será una herramienta de vital importancia para las estrategias de seguridad de los Estados (Álvarez & Ramírez, 2020).

No obstante, se han mencionado los retos y los desafíos de la humanidad en las próximas décadas, las cuales pueden considerarse desalentadoras; sin embargo, el ser humano tiene la característica de ser resiliente, de adaptarse y superar adversidades cuando busca la colectividad hacia un bien común (Harari, 2015), por lo cual no se debe perder la esperanza, siempre y cuando la humanidad cambie su comportamiento, por ejemplo, en cuanto al uso de la tecnología para su evolución adoptando estrategias para mitigar el impacto del cambio climático y construyendo barreras para evitar una autodestrucción nuclear.

Conclusiones

Las dos guerras mundiales, por su connotación y su impacto en las relaciones internacionales, son los eventos mediante los cuales se analizaron los cambios sociales que ha tenido la humanidad desde entonces. Por tanto, la guerra, como uno de los medios que ha establecido el ser humano para relacionarse a lo largo de la historia, no ha dejado, desde entonces, de ser un elemento con resultados trágicos para la propia especie.

Si bien es cierto que a partir de las guerras se han creado ciudades y naciones, también otras han dejado de existir por los intereses territoriales; poder y, paradójicamente, paz, que han desarrollado los seres humanos a lo largo de la vida. En ese sentido, ha sido la violencia la que ha trazado las estrategias de las guerras que han impactado a los propios individuos.

La caída del Muro de Berlín constituyó un punto de inflexión entre la guerra como amenaza tradicional, la aparición de nuevas amenazas a la seguridad y las respuestas, precisamente, en materia de seguridad y defensa. Por lo tanto, la última década del siglo XX ha repercutido significativamente, al punto de que el concepto de seguridad dejó de dar esa respuesta a la multiplicidad y la proliferación de amenazas, lo que motivó para ampliar el sentido de la seguridad a nuevos enfoques.

En el presente documento se analizó el concepto *orden mundial*; si bien es cierto que este fue pronunciado en 1918, eventos predominantemente violentos, como la guerra y las amenazas, han sido excusa para replantear una y otra vez "un nuevo orden mundial". Lo cierto es que en pleno siglo XXI, esos nuevos órdenes mundiales delimitan los retos y los desafíos que enfrenta la humanidad

desde las primeras décadas. Uno de los resultados de lo anterior se plasmó en el último apartado, con la formulación de once retos con los que debe lidiar el ser humano en la presente centuria.

Además de lo anterior, el análisis del orden mundial que se vivió en los siglos XX y XXI, en el marco de las relaciones internacionales, evidencia una lucha de intereses por varios actores en el sistema global contemporáneo, lo cual permite vislumbrar, tras ello, las nuevas amenazas que se desenvuelven en todos los escenarios del planeta, de manera que las estrategias de seguridad para combatir dichas amenazas pueden ser insuficientes.

Por lo anterior, y en relación con las RR. II., el protagonismo en el planeta no es de uno solo ni de algunos cuantos. Por el contrario, actualmente hay una gran cantidad y diversidad de actores estatales, supranacionales, organizaciones privadas, tecnológicas e industriales, así como organizaciones terroristas y criminales, además de individuos; todos, con acceso a la economía y al poder global.

Terminados el siglo XX y la complejidad de la última de sus décadas, junto con el comienzo de la presente centuria, con los ataques del 9-11, se visibilizó un punto de inflexión, en el cual la presente investigación tomó como oportunidad los planteamientos de la declaración de las Américas sobre seguridad multidimensional de la OEA en 2003, y a través de la observación y la búsqueda de otras fuentes, como la ONU, la UNODC y la OTAN, para hacer un análisis documental con el objeto de determinar cuántas y cuáles son las nuevas amenazas a la seguridad, y que se suman a las tradicionales, de la guerra o los conflictos internacionales.

El resultado de esta investigación arrojó un total de 24 nuevas amenazas que afectan al planeta, pero, particularmente, al entorno regional del hemisferio americano, lo cual deja abierta la inquietud para futuras investigaciones sobre la exploración a escala mundial. Además de lo anterior, también se planteó la relación que pueden tener las nuevas amenazas a la seguridad con el uso malintencionado del ciberespacio, el cual puede potencializar cuanta estrategia terrorista y criminal se proponga la maldad, y ello hace más compleja aún las respuestas en seguridad que debe plantear lo supranacional con efectos hacia lo estatal y, en consecuencia, con lo humano. Así pues, y como hallazgo de la presente investigación, se evidencia y se confirma que el sistema internacional sufre por la complejidad de las nuevas amenazas descritas en este documento.

Lo cierto es que el terrorismo, así como el acceso, la posesión y el uso de armas de destrucción masiva, la DOT, el problema mundial de las drogas, el lavado

de activos, el tráfico ilícito de armas de fuego, la trata de personas y la corrupción, fueron las nuevas amenazas más citadas por las fuentes, seguidas por los ataques a la seguridad cibernética, particularmente, lo que, a su vez, permite correlacionar todos los aspectos tratados a lo largo del tema de las amenazas, además de la revisión al documento de Anepe, el cual marca un punto relacional importante, respecto a las amenazas planteadas y la problemática en el ámbito regional.

La mutación a nuevas amenazas ha permeado las barreras de seguridad que tienen los Estados, lo cual los obliga a pactar y apostar por una seguridad colectiva y cooperativa, donde la única solución a dichos problemas no es el poder militar, sino, además, la inclusión de todas las instituciones privadas y públicas de los Estados, teniendo como premisa los intereses de cada nación, desde la orientación y la organización que puedan dar los órganos supranacionales. Asimismo, cabe destacar que la tecnología ha sido y seguirá siendo un aspecto de importancia para la seguridad del entorno global, donde el acceso a la información en tiempo real, puede ser una ventaja o una desventaja en la escena internacional: por ejemplo, el uso de las redes sociales ha sido uno de los mecanismos de grupos terroristas para generar miedo a la sociedad y generar un impacto negativo al sistema internacional.

Finalmente, el trabajo desarrollado a lo largo de los dos primeros apartados permitió la configuración del último, en el cual se pudo dar cuenta de los retos y los desafíos a los que se expone la humanidad en el siglo XXI, aun faltando muchas décadas para su culminación. El resultado de estos once retos propone replantear aspectos importantes, como el cooperativismo en materia de seguridad, la peligrosidad de las armas de destrucción masiva y la contención imperativa del terrorismo, así como la negación del acceso de las estructuras terroristas y criminales al ciberespacio. De igual manera, el necesario control del desarrollo tecnológico en todas las partes del mundo, a fin de no caer en la producción de tecnologías disruptivas con fines destructivos de los seres humanos ni de la naturaleza en general. Por último, y aunque en algunos apartes no considerado una amenaza, están el control y la anticipación de los efectos del cambio climático que sufre el planeta desde décadas atrás.

Las características de fábrica que poseía la Tierra desde su origen son imposibles de reversar. Las nuevas amenazas y una tecnología disruptiva pueden alcanzar los efectos devastadores para la humanidad que esta, en suma, no quisiera presenciar.

Referencias

Aguilera, P., Rodríguez, G., González, R., Miranda, P., & Tassara, C. (2012). *Debates sobre Cooperación Internacional para el Desarrollo*. Escuela Latinoamericana de Cooperación Internacional para el Desarrollo, Convenio Universidad de San Buenaventura Seccional Cartagena, Universidad del Norte y Universidad de Pavía (Italia).

Álvarez Calderón, C. E. (Ed.). (2018). *Escenarios y desafíos de la seguridad multidimensional en Colombia*. Escuela Superior de Guerra. https://doi.org/10.25062/9789585652835

Álvarez Calderón, C. E., & Ramírez Pedraza, Y. E. (2020). La cuarta revolución y la era de la inteligencia artificial: Implicaciones en la seguridad y el trabajo. En *Enfoques y gestión en Seguridad Integral* (pp. 209-237). Escuela de Posgrados de la Fuerza Aérea Colombiana.

Álvarez Calderón, C. E., & Rodríguez Beltrán, C. A. (2018). Ecosistemas criminales. *Revista Científica General José María Córdova, 16*(24), 1-30. https://doi.org/10.21830/19006586.352

Álvarez, C., Rosanía, N., Sánchez, D., & Jiménez, G. (2018). Seguridad y defensa: conceptos en constante transformación. En C. Álvarez (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 29-84).10.25062/9789585652835.01

Álvarez, C., Santafé, G., & Urbano, O. (2017). Metamorphosis Bellum: ¿Mutando a guerras de quinta generación? En C. Álvarez (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 145-248). 10.25062/9789585652835.03

Banegas Alfaro, A. (2017). ¿Existen estrategias para combatir las amenazas multidimensionales en la región? *Revista Política y Estrategia, 129*, 89-120. https://doi.org/10.26797/rpye.v0i129.72

Banegas, A. (2017). *Estrategias para combatir las amenazas multidimensionales en la región*. Academia Nacional de Estudios Políticos y Estratégicos (Anepe).

Barbe, E. (1987). El papel del realismo en las relaciones internacionales (La teoría de la política internacional de Hans J. Morgenthau). *Revista de Estudios Políticos (Nueva Época), 57, 149-176*.

Barbe, E. (1989). El estudio de las relaciones internacionales. ¿Crisis o consolidación de una disciplina? *Revista de Estudios Políticos (Nueva Época) (65), 173-196*.

Bartolomé, M. (2019). Amenazas y conflictos híbridos: características distintivas, evolución en el tiempo y manifestaciones preponderantes. *URVIO. Revista Latinoamericana de Estudios de Seguridad, 25*, 8-23. 10.17141/urvio.25.2019.4249

Biblioteca Virtual en Salud-DeCS. (2022). *Amenaza*. https://decs.bvsalud.org/es/ths/resource/?id=34663

Blackwell, A. (2011). *Cuadragésimo noveno Período Ordinario de Sesiones de la CICAD* [Discurso. Palabras de Adam Blackwell, Secretario de Seguridad Multidimensional, en la ceremonia de Clausura de CICAD 49]. http://www.oas.org/en/sms/docs/speeches/ab_speech_2011_05_06.pdf

Blackwell, A. (2015). Multidimensional security: "facing new threats". *Seguridad, ciencia y defensa*, 153-159.

Blin, A., & Marín, G. (2013). *Diccionario del poder mundial*. Aún Creemos en los Sueños. https://tinyurl.com/4bfdkjwx

Bouthoul, G. (1971). *La guerra*. Oikos-Tau S. A.

Burkett, P. (2020). ¿Un punto de inflexión eco-revolucionario? *Revista Internacional de Salarios Dignos, 2*(01), 15.

Buzan, B., & Waever, O. (2003). *Regions and powers: The structure of international security*. Cambridge University.

Castillo, J. C. P. (2019). *Nuevos roles de las Fuerzas Armadas ante las nuevas amenazas trasnacionales y de seguridad ambiental* [Tesis]. http://hdl.handle.net/10654/35892.

Cataldo, H. G. (2008). Platón, Aristóteles y el siglo IV. *Byzantion Nea Hellás*, (27), 1-15.

Chillier, G., & Freeman, L. (2005). *El nuevo concepto de seguridad hemisférica de la OEA: Una amenaza en potencia*. WOLA. https://www.wola.org/sites/default/files/downloadable/Regional%20Security/past/El%20nuevo%20concepto%20de%20seguridad_lowres.pdf

Chinome Soto, G. A. (2017). *Seguridad multidimensional, fundamento de la estructuración de la defensa y seguridad nacional en Colombia* [Tesis]. http://hdl.handle.net/10654/17074.

Clausewitz, C. V. (2005). *De la Guerra*. La Esfera de Libros.

Council of the European Union, General Secretariat of the Council. (2009). *Estrategia europea de seguridad: Una Europa segura en un mundo mejor*. Publications Office. https://data.europa.eu/doi/10.2860/14070

Dos Santos, T. (2020). *Construir soberanía: Una interpretación económica de y para Amércia Latina*. Clacso.

Estado Mayor de la Defensa. (2019). *PDC-00 Glosario de terminología de uso conjunto*. Estado Mayor de la Defensa de Madrid.

Fazio Vegoa, F. (2006). Globalización y relaciones internacionales en el entramado de un naciente tiempo global.pdf. *Análisis Político, 19*(56), 51-71. https://revistas.unal.edu.co/index.php/anpol/article/view/46287

Fernández Luzuriaga, W., & Olmedo González, H. (2018). Conflictividad y órdenes mundiales: La Paz de Westfalia y la inauguración del sistema internacional contemporáneo. *Crítica Contemporánea*, (8), 48-75.

Fernández-Montesinos, F. A. (2011). *Entender la guerra en el siglo XXI*. Editorial Complutense.

Figueroa Rubio, P. (2013). Estrategias de seguridad en new concepts on international security. It' s impact on. *Estudios de Seguridad y Defensa, 2*, 17-38.

Font, T., & Ortega, P. (2012). Seguridad Nacional, Seguridad Multidimensional, Seguridad Humana. *Papeles de relaciones ecosociales y cambio global, (119)*, 161-172. https://tinyurl.com/mrx697d7

Griffiths, J. (2009). Chile y los desafíos globales de seguridad. *UNISCI Discussion Papers*, (21), 14-26. https://tinyurl.com/5n6sw76y

Guillén, M. F. (2020). Más móviles que inodoros. *En 2030 Viajando hacia el fin del mundo tal y como lo conocemos* (pp. 229-268). Planeta.

Harari, Y. N. (2015). El secreto del éxito. En De animales a dioses (cap. 13). Penguin Random House.

Harari, Y. N. (2018). *Las 2 habilidades más importantes para el resto de su vida. Yuval Noah Harari sobre la teoría del impacto* [Entrevista]. YouTube. https://www.youtube.com/watch?v=x6tMLAjPVyo

Hernández, S. (2008). La teoría del realismo estructuralista y las interacciones entre los estados en el escenario internacional. *Revista Venezolana de Análisis de Coyuntura, XIV*(2), 13-29. https://www.redalyc.org/articulo.oa?id=36414202

Instituto Español de Estudios Estratégicos (Ed.). (2010). *Ciberseguridad: Retos y amenazas a la seguridad nacional en el ciberespacio*. Ministerio de Defensa.

IPCC. (2019). *Calentamiento global de 1,5 °C: Informe especial del IPPC sobre los impactos del calentamiento global. Grupo Intergubernamental de Expertos sobre el Cambio Climático*. https://tinyurl.com/yfkra24h

Jiménez, F. (2019). Cartografías de paces: las etapas de los estudios de paz. En D. Moreira, F. Jiménez & R. Beltrán (Eds.), *Gestión de conflictos* (pp. 123-158). Dykinson.

Kaldor, M. (2012). *New and old wars organised violence in a global era* (3.a ed.). Polity Books.

Keegan, J. (2014). *Historia de la guerra*. Turner Publicaciones.

Keohane, R. (1993). Teoría de la Política Mundial: El Realismo Estructural y lo que va más allá de él. En *Teoría de la Política Mundial* (pp. 57-107). https://tinyurl.com/3rwjc9ck

Koprinarov, L. (2013). La guerra en la paz: El uniforme militar y los preparativos antropológicos para la guerra. *Thémata, 48*, 143-151. https://doi.org/10.12795/themata.2013.i48.12

Matis, J., & Hoffman, F. (2005). Future warfare: The rise of hybrid wars. *Proceedings Magazine, 132*(11). https://tinyurl.com/nwmsb9yr

McLennan, M., & Group, S. (2021). *The global risks report 2021* (16th Ed.). World Economic Forum.

Observatorio Internacional de Estudios sobre el Terrorismo (OIET). (2020). *Anuario del terrorismo yihadista 2019*. COVITE. https://tinyurl.com/yc65ex4w

Observatorio Internacional de Estudios sobre el Terrorismo (OIET). (2021). *Anuario del Terrorismo Yihadista 2020*. COVITE. https://tinyurl.com/4zujkf47

Office of the Director of National Intelligence. (2021). *Annual threat assessment of the us intelligence community. ATA*. https://tinyurl.com/2uy49fjz

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2021). Inicio [sitio web]. https://www.unodc.org/unodc/es/index.html

Olabe, A., & González, M. (2008). Cambio climático, una amenaza para la seguridad global. *Política Exterior, 22*(124), 175-185.

Olaya, S., Godoy, L. F., & Mejía Lagos, A. (2007). El papel de la OEA en la seguridad hemisférica -Evolución y desafíos actuales. *OPEC Observatorio de Política Exterior Colombiana*, 7, 11.

Organización de Estados Americanos (OEA). (2003). *Declaración sobre seguridad en las Américas*. OEA.

Organización de Estados Americanos (OEA). (2020). *Promoción de la seguridad hemisférica: Un enfoque multidimensional*. AG/doc.5698/20 rev. 2. Asamblea General de la OEA. https://tinyurl.com/mwb583m8

Organización de Naciones Unidas (ONU). (2018). *Asamblea General. A/72/840. Actividades del sistema de las Naciones Unidas para la aplicación de la Estrategia Global de las Naciones Unidas contra el Terrorismo*. https://www.mpf.gob.ar/sait/files/2019/08/7-_A-72-840__2018_.pdf

Organización de Naciones Unidas. (ONU). (2020, 22 de enero). *La guerra, el cambio climático, la desconfianza en la globalización y la tecnología nos amenazan*. https://news.un.org/es/story/2020/01/1468371

Organización de Naciones Unidas (ONU). (2021a). *Amenazas transnacionales. Naciones Unidas y el Estado de Derecho. Hacia un mundo justo, seguro y pacífico regido por el estado de derecho*. https://tinyurl.com/4rx2xmkz

Organización de Naciones Unidas (ONU). (2021b). *Declaración y resoluciones aprobadas por la Asamblea General (AG/doc.5717/20)*. Naciones Unidas.

Orozco Carmona, S. (2014). Actores, estructura y proceso del orden político internacional contemporáneo. *Analecta política, 4*(6), 99-120.

Patiño, R. A. (s. f.). *Neorrealismo y Neoliberalismo en las Relaciones Internacionales*. https://xdoc.mx/preview/neorrealismo-y-neoliberalismo-en-las-relaciones-5f35a-6b8a97c3

Pereyra, G. D. (2015). El estudio de la identidad en las Relaciones Internacionales. El constructivismo como "solución" teórica temporal. *Enfoques, XXVII* 1, 127-142.

Pozo, A. M. (2010). *Las guerras globales*. Universitat Jaume.

Ramírez, Y., & Bolívar, J. (2018). Consolidación multidimensional del territorio, hacia un concepto de seguridad para el posacuerdo. En C. Álvarez (Ed.) *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 555-590) 10.25062/9789585652835.03

Rosa, H. (2011). Aceleración social: Consecuencias éticas y políticas de una sociedad de alta velocidad desincronizada. *Revista Persona y Sociedad, XXV*(1), 9-49.

Sanahuja, J. A. (2020). ¿Bipolaridad en ascenso? *Foreign Affairs Latinoamérica, 20*(2), 76-84.

Schneider, Y. (2015). The new security: Trends in the study of security in international relations in the post-cold war era. *The Institute for National Security Studies*, (195), 31-46. https://tinyurl.com/mrydx372

Tello, A. P. (2000). Conceptos de seguridad y defensa. *Relaciones Internacionales 9(19)*. https://revistas.unlp.edu.ar/RRII-IRI/article/view/1672

UNODC. (2021). *UNODC Strategy 2021-2025*. https://www.unodc.org/unodc/strategy/index.html

Uribe, D. (2014). *Guerras del siglo XX*. [Video]. YouTube. https://tinyurl.com/2p8hzz24

Vargas Hernández, J. G. (2010). El realismo y el neorrealismo estructural. *Estudios Políticos, 9*. https://doi.org/10.22201/fcpys.24484903e.2009.0.18777

Waltz, K. N. (1988). The origins of war in neorealist theory. *Journal of Interdisciplinary History, 18*(4), 615. https

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).

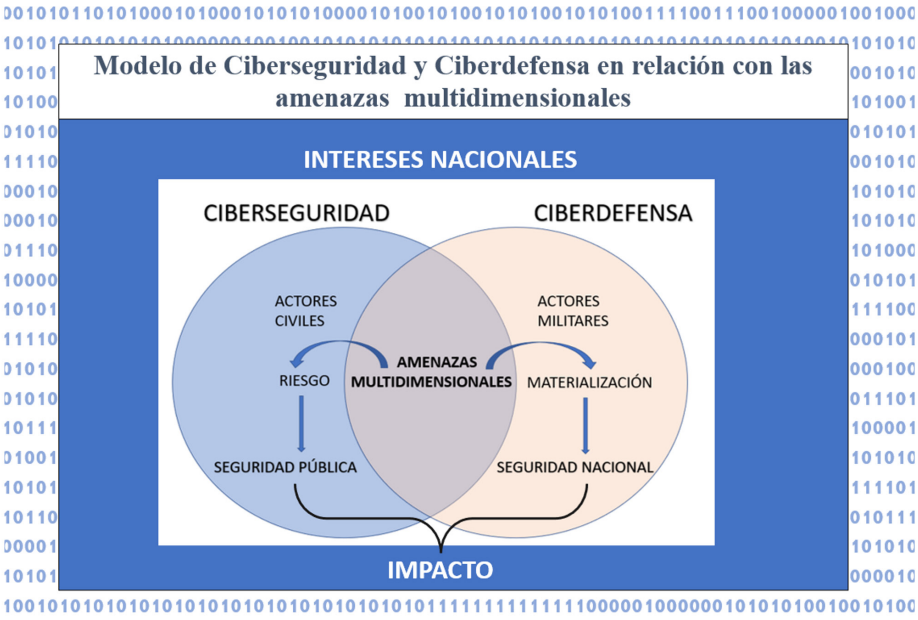
De este modo, una capacidad con la que el Estado colombiano debe contar para combatir y contener las amenazas multidimensionales en el dominio aéreo identificadas en el primer acápite, y descritas en la figura 1, debe ser la modernización de los medios aéreos que hacen parte del sistema de defensa aérea 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.

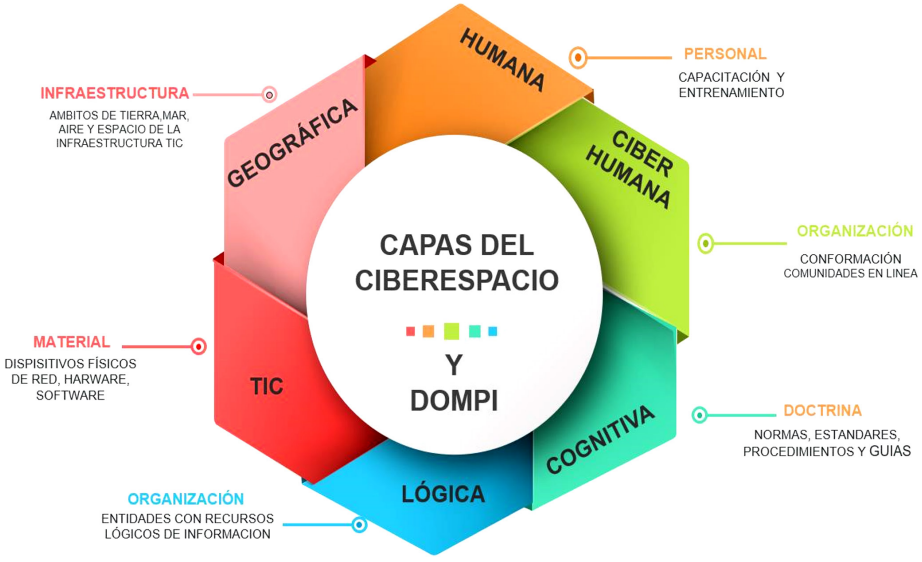
Conviene distinguir cómo en este modelo intervienen distintos actores del ámbito de la ciberseguridad; a saber: civiles que tienen la responsabilidad de proteger infraestructuras al interior del sector privado, y actores estatales a cargo de la protección de los derechos y las libertades de los ciudadanos 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.

Capítulo 4

Amenazas y desafíos multidimensionales para la ciberseguridad y la ciberdefensa, en los dominios espacial y ciberespacial*

DOI: https://doi.org/10.25062/9786287602106.04

José Luis Martínez Díaz
Javier Hernando Conde Mesa
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: Este capítulo busca identificar y analizar las amenazas y desafíos más relevantes para la ciberseguridad y ciberdefensa que afectan el dominio espacial y ciberespacial. Para ello, se enfatizó en la ciberseguridad como el mecanismo que asegura el acceso permanente al espacio exterior y el agente protector ante las amenazas cibernéticas elaborando una clasificación descriptiva de su impacto e identificando las vulnerabilidades de mayor relevancia. Asimismo, se describió el panorama mundial y nacional en materia satelital, así como sus tendencias, y se plantearon estrategias de mitigación del riesgo y contención de amenazas. Lo anterior contribuye a generar conciencia sobre los peligros cibernéticos a los que se hallan expuestos los operadores y usuarios de estas tecnologías y, asimismo, facilita la generación de nuevo conocimiento en materia doctrinal espacial frente a la nueva responsabilidad asumida en 2020 por la Fuerza Aérea Colombiana, con la inclusión de una nueva misión, denominada *Contrapoder Espacial*.

Palabras clave: Ciberamenazas, ciberespacio, ciberseguridad, riesgo cibernético, sistemas espaciales.

* 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.

José Luis Martínez Díaz
Teniente Coronel de la Fuerza Aérea Colombiana. Piloto militar instructor de ala fija y rotatoria. Administrador aeronáutico. Msc. Ingeniería Aeroespacial y Aviación de la Universidad Tecnológica de Melbourne. Magíster en Ciberseguridad y Ciberdefensa de la ESDEG. Comandante del Grupo de Entrenamiento de Vuelos de la Escuela Militar de Aviación "Marco Fidel Suarez". ORCID: https://orcid.org/ 0000-0003-4821-2144 - Contacto: jose.martinezd@fac.mil.co

Javier Hernando Conde Mesa
Teniente Coronel de la Reserva Activa de la Fuerza Aérea Colombiana. Administrador aeronáutico. Magíster en Educación de la Universidad Militar Nueva Granada. Docente ocasional e investigador del Grupo Masa Crítica, en la ESDEG. ORCID: https://orcid.org/0000-0001-7152-9399- Contacto: Javier.conde@esdeg.edu.co

Citación APA: Martínez Díaz, J. L., & Conde Mesa, J. H. (2022). Amenazas y desafíos multidimensionales para la ciberseguridad y la ciberdefensa, en los dominios espacial y ciberespacial. En F. Baquero Valdés (Ed.), *Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano* (pp. 153-208). https://doi.org/10.25062/9786287602106.04

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

Para el caso colombiano, el desarrollo del dominio espacial, como una capacidad autónoma y sostenible, ha tenido un panorama incierto y limitado por el contexto político, en la medida en que tiene políticas de gobierno, pero carece de políticas de Estado aplicables al dominio espacial de largo plazo que permitan a los actores gubernamentales delimitar el desarrollo y la explotación de esta capacidad como un interés nacional (Álvarez & Corredor, 2019).

Pese a lo anterior, la FAC posee un satélite autónomo de observación de la Tierra: el FACSAT-1, lanzado en noviembre de 2018, y el cual ha generado un nuevo campo de desarrollo sobre el ámbito espacial en el país, en cuanto a los principios de mecánica orbital, misiones espaciales, ingeniería de sistemas, sensoramiento remoto y uso de *software* satelital, entre otros temas, los cuales apalancan la obtención de capacidades en ciencia y tecnología para generar nuevo conocimiento, y llevan así a desarrollar doctrina de operación y mantenimiento de segmentos espaciales y terrestres.

Asimismo, diversas organizaciones en el ámbito nacional poseen y operan estaciones terrestres, y gracias a estos obtienen el acceso a productos y servicios de proveedores externos, como lo son las comunicaciones, las imágenes para propósitos meteorológicos o los análisis de terreno y control de tráfico aéreo. Dichos sistemas esenciales de información requieren estar protegidos de amenazas cibernéticas, para así asegurar su disponibilidad permanente, su integridad y su confidencialidad, y para no degradar la confiabilidad en el desempeño de los sistemas y los activos estratégicos del ámbito espacial.

Por tal motivo, con respecto al dominio ciberespacial, es indispensable reconocer el papel que dicho dominio desempeña en la transformación del mundo, suscitada por el advenimiento de la Revolución Industrial 4.0, la era de la digitalización y la masificación de tecnologías en todos los sectores, los modelos de negocios y las cadenas productivas (Barleta et al., 2020). Nada de ello ha pasado desapercibido para la transformación del sector público, ni para la seguridad nacional ni, por supuesto, para las amenazas asociadas, en un mundo cada vez más globalizado e interconectado a través del procesamiento de la información transitando por el ciberespacio.

Cabe denominar al poder ciberespacial como una herramienta para propender por la defensa de los derechos a la información y a la comunicación. Las operaciones cibernéticas no son de carácter tangible, pero actúan de manera transversal a los demás dominios, a todos los cuales puede afectar, y en todos los cuales pueden manifestarse de manera perceptible afectando los activos, los recursos y los intereses nacionales (Vargas, 2014). Asimismo, y de acuerdo con el Centro Cibernético Conjunto y los Centros de Operaciones de las Unidades Cibernéticas de las Fuerzas Militares, las amenazas se encuentran en constante evolución, lo que se evidencia a través del empleo de técnicas estructuradas y dirigidas contra las infraestructuras Críticas Cibernéticas Nacionales (ICCN) —de las cuales los activos espaciales hacen parte—, y se corrobora al detectar y mitigar eventos que provienen de las denominadas *amenazas persistentes avanzadas*[1] (Comando Conjunto Cibernético, 2021).

Sin embargo, el ataque a centros de gravedad afecta no solo a los mandos militares y las organizaciones estatales, sino a todos aquellos sectores indispensables para el normal desarrollo de la sociedad (i.e. comercio, educación, medios de comunicación, servicios financieros y salud, entre otros), lo que convierte a la seguridad y defensa del espacio y el ciberespacio en un objetivo estratégico para garantizar la seguridad nacional (Vargas, 2014). Por consiguiente, los esfuerzos por contener los riesgos y sus potenciales consecuencias derivadas de este fenómeno no recaen en un asunto netamente militar y, sin duda, la ciberseguridad constituye un desafío, en la medida en que urge la cooperación de todos los actores inmersos en este dominio (Llongueras, 2011).

1 Las amenazas persistentes avanzadas consisten en una técnica de intrusión a un sistema informático infringiendo las medidas de seguridad, con el propósito de extraer información esencial, con el atacante manteniéndose indetectable durante el mayor tiempo posible. Es una actividad estrechamente relacionada con el ciberespionaje (Centro Criptológico Nacional, 2020).

En cuanto a la interacción entre el dominio espacial y el ciberespacial, es importante resaltar que todos los sistemas espaciales dependen de las capacidades cibernéticas, incluyendo el *software*, el *hardware*, otros componentes y su infraestructura de red, por lo que cualquier amenaza al sistema de control de un satélite o al sistema de red representa un desafío a los activos estratégicos.

Con respecto a los demás dominios (aéreo, terrestre, y marítimo), y tomando en cuenta la experiencia llevada a cabo por la Organización del Tratado del Atlántico Norte (OTAN) (OTAN, 2019), las misiones y las operaciones que se llevan a cabo requieren la provisión de datos y servicios asociados a la explotación del espacio. La dependencia crítica del espacio ha dado lugar a nuevos riesgos cibernéticos, que podrían afectar, y de manera desproporcionada, el éxito de una misión. La necesidad de invertir en medidas de mitigación y en la resiliencia de los sistemas espaciales es clave para lograr protección en todos los dominios (OTAN, 2019).

Planteadas las relaciones del empleo del poder ciberespacial, se evidencia cómo hay diferentes factores de inestabilidad sobre el dominio espacial, y ello establece la necesidad de que haya un interés nacional permanentemente direccionado a mantener a la nación protegida de los riesgos asociados a dichos dominios y de su estrecho vínculo con el normal funcionamiento de las infraestructuras críticas.

El incremento y la mutación de las amenazas plantean grandes retos y desafíos que obligan al Estado y a las organizaciones comprometidas en permanente vigilancia a formular estrategias para la identificación, la detección, la contención y su respectiva negación. Es importante mantener una revisión continua de las medidas de protección en materia de ciberseguridad y ciberdefensa, de modo que se facilite la proyección del poder espacial y ciberespacial en el Estado colombiano, como una estrategia nacional para combatir y contener las amenazas multidimensionales que afectan la supervivencia y el interés nacionales.

En consecuencia con lo anterior, se plantea la siguiente pregunta producto de investigación: *¿Cuáles son las amenazas y los desafíos multidimensionales para la ciberseguridad y la ciberdefensa, en los dominios espacial y ciberespacial, que afectan los intereses nacionales del Estado colombiano?*

Es así como el crecimiento en el número de ataques cibernéticos a los activos satelitales ha suscitado un mayor interés por la seguridad cibernética a nivel mundial, siendo el entorno digital el medio por el cual se desarrollan las actividades socioeconómicas asociadas al uso del espacio exterior. Esto expone a las

organizaciones a amenazas cibernéticas por parte de los actores involucrados que aprovechan el creciente desarrollo de las tecnologías espaciales.

Con el fin de abordar la problemática expuesta, este capítulo tiene como propósito la identificación y la caracterización de las principales ciberamenazas que afectan los sistemas espaciales, en el marco de la nueva era espacial y el entorno digital marcado por las tecnologías disruptivas, la interconexión de redes y el creciente mercado satelital, abordando la interacción y la interdependencia entre el dominio espacial y el ciberespacial, el panorama satelital global y la proyección colombiana en el espacio.

El espacio y el ciberespacio: una estrecha relación que se afianza en el tiempo

Historia y evolución del dominio espacial

De acuerdo con Ley et al. (2009), el desarrollo y la conquista del dominio espacial son también la historia del cohete, que se remonta no solo al lanzamiento del primer satélite artificial ruso —el *Sputnik*—, en 1957, sino a una serie de previos esfuerzos científicos y actividades de desarrollo tecnológico que dieron paso a la materialización de este gran hito. Por lo anterior, y para comprender la evolución del desarrollo espacial, resulta pertinente dividir en varias etapas el marco de tiempo (OCDE, 2019).

En la primera de dichas etapas es necesario nombrar al ruso Hermann Ganswindt: uno de los primeros en formular la viabilidad técnica de una nave espacial y su diseño preliminar. Igualmente, cabe citar a su compatriota Konstantin Tsiolkovsky, llamado 'El padre de la Cosmonáutica', con sus aportes a las teorías de propulsión. Por otro lado, la participación del estadounidense Robert Goddard, conocido, a su vez, como 'El Padre de la Tecnología de Cohetes' contribuyó a sentar las bases de la cohetería de varias etapas. De vuelta en el continente europeo, hace su aparición el alemán Hermann Oberth, quien es considerado *pionero de los vuelos espaciales*, mientras que su compatriota Wernher von Braun, su alumno más talentoso, afianzó la generación del conocimiento pionero que abrió paso al lanzamiento de misiles balísticos, con el prototipo V2, en 1942.

Consecuentemente, en el marco de la posguerra se inició la *carrera espacial*, por el desarrollo de los misiles balísticos intercontinentales, entre 1943 y 1957, lo que, a su vez, dio paso a la puesta en órbita del primer satélite ruso: el *Sputnik*.

Esto abrió el camino al uso militar de las nuevas capacidades para el espionaje, la exploración robótica y la operación de naves tripuladas, hasta el fin del programa *Apollo*, en 1972 (Llongueras, 2011).

Posteriormente, en una segunda etapa, a partir de 1973, se desarrollaron los transbordadores estadounidenses y rusos, y con ellos, el lanzamiento de las primeras estaciones espaciales (e.g., *Skylab* y *Salyut*), los sistemas de posicionamiento global (e.g., *Glonass* y *GPS*) (Hutchins, 2016) y la participación de los ámbitos civil y comercial en actividades de observación de la Tierra y las telecomunicaciones, al igual que la aparición de nuevos actores, como Europa, Japón y China (OCDE, 2019; Flórez, 2020).

A partir de 1987 surgió una tercera fase, con la segunda generación de estaciones espaciales (e.g., *MIR* e *ISS*), y entonces este dominio desempeñó un papel más protagónico en aplicaciones espaciales militares, en el marco de la cooperación internacional y, paralelamente, vio un mayor desarrollo de aplicaciones civiles y comerciales a un alto costo, pero con extensos tiempos de vida útil (e.g., los sistemas *Landsat* y *Spot Image*, y la televisión satelital). Asimismo, de acuerdo con Bichler (2015), a finales del siglo XX se amplió la serie de actores partícipes del mercado satelital, mediante la transferencia tecnológica, legado de la Guerra Fría y de la incursión del ciberespacio, al fusionar los datos espaciales con las redes de datos globales, gracias a lo cual se logró el uso compartido de la información y se facilitó la toma de decisiones; todo lo anterior, es lo que la evolución de la historia espacial ha denominado *La antigua era espacial* (OCDE, 2019; Manulis et al., 2020).

Tras la revolución digital comenzando el siglo XXI, se dio un cuarto paso como resultado de un proceso de transformación, designado la *nueva era espacial*, que, junto al ritmo acelerado de la globalización de las cadenas de valor, internet y su aplicación en sistemas espaciales, ha permitido una nueva generación de sistemas ultraterrestres, los cuales han experimentado una miniaturización de sus componentes, impulsada por la innovación en microelectrónica, la computación y los nuevos materiales (OTAN, 2019). Estos cambios han reducido costos y promovido nuevas capacidades para las organizaciones, tanto públicas como privadas, que incluyen sistemas para la navegación de aérea y marítima, la observación de la Tierra, el internet de las cosas (en inglés, IoT, por las iniciales de *Internet of Things*) y las telecomunicaciones. Como consecuencia, se ha desatado una rivalidad tecnológica, fundamentada en los beneficios de poseer capacidades estratégicas del dominio espacial (Fuerza Aérea Colombiana (FAC), 2020a).

Desde 2018, el mundo atraviesa por el último ciclo del desarrollo espacial, donde las capacidades de los sistemas informáticos y la dependencia de los sistemas satelitales comprenden una oferta masiva de productos y servicios, en el marco de la nueva generación de sistemas de exploración científica que comprende nuevas estaciones espaciales, expediciones planetarias y misiones robóticas (OCDE, 2019).

Habiendo hecho un breve recorrido histórico, resulta pertinente hacer una distinción de las características, los componentes y las aplicaciones relativas al dominio espacial, que permita más adelante comprender su interacción con el dominio ciberespacial.

Caracterización de los sistemas espaciales

A diferencia del dominio terrestre, el marítimo o el aéreo, el entorno espacial se encuentra libre de un medio que lo circunde; sin embargo, el ambiente de vacío hace vulnerables a las plataformas espaciales, debido a las partículas cargadas y los campos magnéticos y eléctricos, por lo cual requiere de dichas plataformas exigentes especificaciones de diseño para soportar las temperaturas extremas, los diferenciales de presión y la alta radiación, todo lo cual varía dependiendo de las distancias orbitales respecto a la Tierra, y que abarcan la ionósfera y magnetósfera (Fuerzas Militares de Colombia (FF. MM.), 2018).

Dado lo anterior, existen diferentes tipos de órbitas: la de *baja altura* (LEO) comprendida de los 200 km a los 1.600 km, e ideal para aplicaciones de observación de la Tierra con menor latencia en las comunicaciones, y con inferiores especificaciones de potencia por su cercanía al planeta. También se encuentran las órbitas *de mediana altura* (MEO), comprendida de los 5.000 km a los 22.000 km, y las órbitas *polares*, que describen una órbita de 90° con respecto al ecuador. Por otro lado, están las *geoestacionarias*, con un ángulo cero de inclinación, y que deben orbitar, aproximadamente, a 35.789 km de altura, eficaces para su uso en comunicaciones y meteorología. Por último, las órbitas *helicosincrónicas* hacen su paso a una determinada latitud terrestre a un mismo tiempo solar (CONPES, 2009; OCDE, 2015; Wang et al., 2016). Por otro lado, estos satélites pueden operar de manera individual cumpliendo una misión específica, en pequeños grupos en una formación, o en una constelación, a fin de brindar una complementaria y permanente cobertura de comunicaciones en tierra (Manulis et al., 2020).

Tomando en cuenta lo anterior, y de acuerdo con la revisión de la literatura existente (CONPES, 2010; Departamento Nacional de Planeación [DNP], 2019a;

OTAN, 2019; FAC, 2020b; Manulis et al., 2020), las capacidades comprenden cinco segmentos: *espacial*, *terrestre*, *de red* o *de enlace de datos*, *lanzamiento* y de *usuario final*. A efectos del presente estudio, se hará énfasis en los tres primeros.

El segmento espacial se compone de una plataforma y de una carga útil, junto con una serie de subsistemas: comunicaciones, posicionamiento, procesamiento y potencia; estos le permiten recibir instrucciones y transmitir datos desde y hacia el sistema terrestre; hoy día existe un alto nivel de industria tecnológica y de personal calificado, el cual ha adoptado un sistema de diseño estandarizado que se prolonga través de todo el ciclo de vida de un satélite durante las etapas de pruebas, validación, lanzamiento, operación y retiro del servicio (Ley et al., 2009), para lo cual existe un segmento terrestre que desempeña un papel fundamental en su control.

El segmento terrestre es el encargado del comando, el control, la telemetría y el procesamiento inicial de datos. Permite la operación rutinaria de la plataforma y la su carga útil, y monitorea su integridad; adicionalmente, lo componen estaciones terrenas, centros de control de misión y redes terrestres que conectan todo el sistema.

Por último, cabe mencionar el segmento denominado *de red*, o *de enlace de datos*, que corresponde al sistema de transmisión y recepción de señales de comunicación a través del uso del espectro electromagnético, y que permite el enlace entre el segmento espacial y el terrestre, para control y monitoreo (FAC, 2020b).

Los mencionados segmentos logran, en operación coordinada, un adecuado acceso al espacio y a su aprovechamiento de bienes y servicios; una dinámica que se ha vuelto fundamental en el progreso de la sociedad, no solo en el ámbito militar, como herramienta de influencia y poder a escala global (Hutchins, 2016), sino también, como un mecanismo de oferta de productos en beneficio de la comunidad, tomando en cuenta la ventaja de la capacidad de recepción y envío de datos desde cualquier punto geográfico, y anulando las barreras terrestres (Flórez, 2020).

Expuesto lo anterior, se catalogan las tecnologías satelitales en seis grandes capacidades militares: *posición y navegación*; *inteligencia, vigilancia y reconocimiento*; *defensa de misiles*; *comunicaciones*; *conciencia situacional*, y *monitoreo ambiental*. Sin embargo, por su gran porcentaje de participación en la oferta satelital, es posible resumir dicha clasificación en solo tres grandes ramas: *comunicación*, *navegación* y *sensores remotos* (CONPES, 2010; OTAN, 2019), las cuales se describirán seguidamente.

Aplicaciones y beneficios de las plataformas satelitales

El campo de la tecnología satelital de las comunicaciones es un sector creciente en la infraestructura global, y que aún no ha sido reemplazo por la tecnología de fibra óptica; se caracteriza por su rapidez y su flexibilidad, y requiere el uso de la órbita geoestacionaria, la cual es un recurso natural escaso y limitado. Sin embargo, en algunos casos opera en la órbita LEO, a fin de servir como retransmisor entre otros sistemas satelitales. De acuerdo con la Organización para la Cooperación y el Desarrollo (OCDE, 2019), existen más de 50 operadores que ofrecen una gran variedad de servicios, de los cuales cabe mencionar tres, por su gran contribución al mercado satelital: servicios fijos (en inglés FSS, por las iniciales de *Fixed Satellite Services*), servicios móviles (en inglés, MSS, por las iniciales de *Mobile Satellite Services*) y servicios de transmisión (en inglés, BSS, por las iniciales de *Broadcast Satellite Services*). Al mismo tiempo, una compleja red de estaciones terrenas robustece la amplia cobertura facilitando la comunicación en áreas remotas con limitada infraestructura, y beneficiando tanto al sector público como al privado (Manulis et al., 2020).

Los sistemas satelitales dedicados a los servicios de navegación proveen información de coordenadas en el marco de referencia global, así como de la medida del tiempo, lo que, paulatinamente, exige un mayor margen de precisión y confiabilidad. Su permanente disponibilidad facilita la creación de nuevos servicios, así como el incremento de la economía global, a través de la mejora en la eficiencia de amplios sectores de economía relacionados con la gestión del tráfico terrestre, marítimo y aéreo, con seguridad y defensa, con el medio ambiente y con servicios personales (civiles y comerciales), y así facilita los procesos logísticos y las cadenas de suministro asociados (Ley et al., 2009). En la actualidad, existen cuatro diferentes sistemas de navegación por satélite con cubrimiento global (GPS, Galileo, Glonass y Beidou), transmitiendo en distintas frecuencias (OCDE, 2015).

La tercera rama en cuestión, referente a los sensores remotos, fue la primera disciplina científica en usar las capacidades espaciales desde 1960, y al igual que las dos anteriores capacidades, ha impulsado la economía global a través de su particular papel, relacionado con el monitoreo de los recursos naturales, con sistemas productivos y con la confrontación de las mayores problemáticas y desafíos actuales (i.e. cambio climático, gestión del riesgo y predicciones, desarrollo urbano, seguridad y defensa, entre otros) (CONPES, 2010); todo ello, en conexión directa con centros de procesamiento, donde genera datos e información

que son distribuidos hoy día a través de arquitecturas basadas en aplicaciones web, y que, finalmente, son recibidos por el usuario final, para la respectiva toma de decisiones. Lo anterior, tomando en cuenta que, por ejemplo, el 75 % de las predicciones climáticas se basan en la información brindada por plataformas satelitales (OCDE, 2015).

Por lo general, existen dos tipos de sensores: *pasivos* y *activos*. La diferencia consiste en que estos últimos son capaces de emitir en su propia frecuencia electromagnética, y así evitan depender de la luz solar y de la afectación de las condiciones atmosféricas existentes, pero con un procesamiento y una capacidad de análisis mucho más complejos y que no han alcanzado, al momento, su madurez tecnológica (CONPES, 2010).

En esta *nueva era espacial*, capital tanto público como privado ha sido atraído por los beneficios que ofrecen desde los pequeños satélites y las microsatélites hasta las megaconstelaciones, lo que, finalmente, se traduce en crecimiento económico. De acuerdo con la OCDE (2019), en 2008 el número de países con satélites registrados en órbita correspondía a un total de 50; trascurrido 2018 creció a 82, y a pesar de que la experticia de cada país y la complejidad técnica de los satélites varían significativamente, sin duda se puede afirmar que estas tecnologías se encuentran a un mayor alcance de las naciones y las organizaciones en relación con su capacidad económica que permite la explotación de las ventajas ofrecidas por el acceso al espacio.

Existen diversos actores y factores dinamizadores del ámbito espacial; por ejemplo, para 2017 Estados Unidos aportaba más de la mitad del presupuesto público invertido a escala global en el espacio, seguido por China, Japón y Francia. Por otro lado, y de manera paralela, más de 500 compañías particularmente originarias de estos mismos países, pero que incluyen a otros muchos, han emergido en los últimos cuatro años ofreciendo capacidades disruptivas de diseño de componentes en impresión 3-D, producción en masa, lanzamiento espacial, oferta de servicios de IoT y analítica de datos; todo ello, a través de procesos de investigación, desarrollo e innovación, donde hay alrededor de 45 agencias espaciales en el mundo que apalancan la ciencia y la tecnología (OCDE, 2019).

Estas iniciativas han sido impulsadas por la globalización, la evolución de las cadenas de suministro, la revolución de las tecnologías digitales, el flujo de datos y el trabajo colaborativo. Por ende, se ha generado, definitivamente, un cambio de paradigmas en el ámbito espacial, un dominio que en el pasado fue protegido tecnológicamente por una cantidad reducida de países, y en el que se ha generado un

ambiente más complejo de cooperación y de competitividad, que, a su vez, ofrece más oportunidades y más beneficios, pero en el que constantemente emergen más riesgos inherentes a las cadenas de valor (OCDE, 2015, 2019).

La funcionalidad del segmento espacial radica en la naturaleza de su carga útil, pero una serie de subsistemas facilitan la apropiada operación de la plataforma a lo largo de su ciclo de vida; generalmente, la arquitectura satelital se compone de cinco elementos: sistema de procesamiento, potencia, comunicaciones, actuadores y sensores (Falco, 2020), lo cual permite, en conjunto, la recepción de señales, la transmisión, la validación, la decodificación y el envío de comandos a otros subsistemas, así como el control, la estabilización y la orientación física del sistema. Asimismo, de acuerdo con Manulis et al. (2020), las fallas asociadas a esos mismos componentes pueden ser originadas por causas naturales, por error humano o, incluso, por estar relacionados con ataques cibernéticos en el marco de la nueva era espacial en un mundo interconectado y expuesto a nuevas amenazas, y en el cual el dominio ciberespacial ha tenido un papel protagónico, que será descrito a continuación.

Desarrollo, evolución e implicaciones del dominio ciberespacial

Este quinto dominio tuvo su origen en Estados Unidos, en 1969, cuando la American Advance Research Projects Agency (ARPA) inició un proyecto de tipo experimental para la interconexión electrónica de computadores remotos, con el propósito de hacer intercambio de información. Así se desarrolló el primer sistema de correo electrónico (Llongueras, 2011). Para 1975, el Ministerio de Defensa del mismo país catalogó el proyecto como una prioridad en sus sistemas de comunicaciones, por lo cual creó dos tipos de redes diferentes: una en la que se mantuviera la confidencialidad de la información militar (MILNET), y otra que apoyara los procesos de investigación asociados a estos nuevos desarrollos (ARPANET) (FAC, 2015).

A mediados de la década de 1980, mediante el desarrollo del proyecto de *software* ENQUIRE, llevado a cabo en el Organización Europea para la Investigación Nuclear (CERN), el centro de investigación científico más grande de Europa, se desarrolló el sistema de gestión de información en red, más conocido como el *World Wide Web* (www). Para 1992, se puso en funcionamiento la primera versión, y un año más tarde fue difundido a los diferentes sistemas operativos, a raíz del éxito obtenido (Llongueras, 2011).

Esta tendencia disruptiva se incorporó gradualmente —tanto al sector público como en el privado— en el área de las comunicaciones, educación, salud y transporte, pero fue el campo militar donde tuvo gran relevancia: por ejemplo, durante la guerra del Golfo Pérsico se emitieron las primeras políticas y directrices frente al dominio cibernético; y la Coalición aprovechó ese nuevo entorno y esas nuevas herramientas en contra del Gobierno iraquí (Llongueras, 2011).

Con el uso de estas innovadoras capacidades, nombradas *ciberarmas*, también nuevas amenazas emergieron, a través de la inyección de códigos dañinos a los sistemas informáticos; una situación que para 2002 alcanzó un nivel de tecnificación en el que los desarrolladores de *software* malicioso lograron una profesionalización en esta actividad, lo que permitió comercializar herramientas de ataque informático, muy efectivas y a un bajo costo (Bejarano, 2011).

Este nuevo entorno condujo a la introducción del término *ciberespacio*, que para 2006 fue catalogado por el Departamento de Defensa de Estados Unidos como "un dominio caracterizado por el uso de la electrónica y del espectro electromagnético para guardar, modificar, intercambiar información a través de los sistemas y redes de la información y las infraestructuras físicas" (Llongueras, 2011, p. 18). Para 2008, el Gobierno estadounidense lo definió, más aún, como "un dominio global dentro del medio de la información compuesto por las interdependientes infraestructuras y redes de la información, incluyendo la Internet, redes de telecomunicaciones, sistemas de computadoras, así como procesadores y controladores" (Llongueras, 2011, p. 18).

Similarmente, en el Manual de Ciberseguridad y Ciberdefensa y Doctrina Básica Aérea, Espacial y Ciberespacial de la Fuerza Aérea Colombiana, así como en otra literatura relacionada, se estableces que existe una interacción entre los ambientes físico y virtual, junto con sus componentes: sus sistemas y sus programas computacionales (i.e. *hardware* y *software*) y sus redes de telecomunicación, para el intercambio de datos e información entre usuarios (FAC, 2015; FAC, 2020a; Lewis et al., 2016; FF. MM., 2018;). Por tanto, es fundamental tener en cuenta dentro de esta definición al *espectro electromagnético*, pues uno de los segmentos espaciales es el relacionado con la transmisión de datos.

A partir de la primera década del presente siglo, los avances en el procesamiento de datos, nanotecnología, inteligencia artificial (en inglés, AI, por las iniciales de *Artificial Intelligence*), computación cuántica e hiperconexión de redes ha dado paso al fenómeno conocido como la *Cuarta Revolución Tecnológica*, término acuñado durante la Feria de Hannover, en 2011, en el que se plantearon

iniciativas para lograr una estandarización de dispositivos y capacidad de conexión automática mediante la filosofía *plug and play*, para así facilitar la conexión digital de componentes (Becerra et al., 2019).

Los sistemas satelitales no han sido a estas transformaciones y tendencias de la tecnología; por consiguiente, se describirá a continuación cómo confluyen los dominios espacial y ciberespacial, y sus relaciones de dependencia, que permitirán conocer posteriormente las amenazas a las cuales se enfrentan los sistemas de infraestructura crítica asociados.

Interacción y dependencia entre el espacio y el ciberespacio

Con el avance de la microelectrónica —donde cada 18 meses un chip dobla su capacidad, y donde el ancho de banda de las comunicaciones se duplica cada 12 meses, y el *software*, a un ritmo de tan solo diez meses—, es comprensible que se aprecien las potenciales capacidades de los sistemas informáticos por sobre los físicos para atender requerimientos técnicos, lo cual permite, en el ámbito espacial, operaciones globales a gran velocidad y de gran alcance, pero igualmente expuestas a los peligros asociados al desarrollo tecnológico, tomando en cuenta que el control y la gestión de la información en el momento adecuado constituye un requerimiento crítico de las organizaciones actuales (Llongueras, 2011).

La anterior apreciación concuerda con la interacción del dominio espacial y del ciberespacial, los cuales, de acuerdo con Livingstone y Lewis (2016), se hallan inextricablemente relacionados, debido a que los activos espaciales provienen de cadenas de suministros globales que, a su vez, requieren periódicamente actualizaciones de *software* y, por ende, conexiones remotas, las cuales pueden llegar a ser vulnerables a ataques cibernéticos. Asimismo, la OTAN (2019) reivindica la importancia de los sistemas espaciales para los dominios tradicionales (terrestre, marítimo y aéreo), pero también resalta la dependencia de los satélites para su funcionamiento con respecto a la tecnología asociada al ciberespacio, y que incluye el uso de *software*, *hardware* y otros componentes digitales, por medio de los cuales pueden emerger amenazas, y así generarse grandes desafíos a los activos críticos nacionales.

Una gran número de sistemas espaciales lanzados a finales de la primera década del siglo XXI lo fueron usando tecnología propia de los tiempos cuando internet apenas si estaba en desarrollo; sin embargo, la tendencia actual, que facilita las operaciones satelitales, marcará el cambio a futuro en el corto plazo (Hamilton, 2020); con ello en mente, a continuación se detallarán los

aspectos más importantes que componen la interacción y las implicaciones para el espacio y el ciberespacio en cuanto al desarrollo del *hardware* y el *software* que componen el segmento satelital y, asimismo, el segmento de tierra.

El desarrollo del *hardware* usado en el espacio debe considerar un alto nivel de tolerancia a las fallas y a las anomalías, a través de un diseño, una producción, una inspección, una cualificación y una aceptación de componentes que se fundamenten en la valoración de riesgos, y que permitan su disponibilidad, su integridad y en especial su confiabilidad bajo los estándares de agencias espaciales. Por lo tanto, se ha observado una evolución en el desarrollo de componentes mecánicos a electrónicos, y de estos últimos, a sistemas basados en *software*.

Esta tendencia, propia de la nueva era espacial, facilita considerablemente el acceso y la interacción de los sistemas espaciales a las tecnologías digitales, pero también trae como resultado una mayor dificultad para la comprensión del *know-how*, dado que la combinación de este conocimiento, desarrollado por diversas disciplinas de alto nivel, yace inmersa en el *software* producido, y en el cual se combinan las diversas complejidades de los lenguajes técnicos (Ley et al., 2009).

A inicios de la primera década del siglo XXI se llevaron a cabo grandes innovaciones tecnológicas en el campo satelital, y hoy día juegan un papel fundamental en ello. En 1999 se definió, por parte de la Universidad de Stanford y el Politécnico de California, la especificación del *Cubesat*, y a partir de este momento se promovió y se incentivó el interés en desarrollar capacidades de manufactura de pequeños satélites, para así reducir costos y tiempo, y ello provocó una revolución en la industria espacial, a través del uso de *componentes tomados del estante*, lo cual se refiere a productos adquiridos en grandes cantidades en el mercado comercial, y que se adaptan para usos específicos. Entre estos avances, se encuentra el desarrollo de la *matriz de puertas lógicas programable en campo* (en inglés, FPGA, (por las iniciales de *Field-Programmable Gate Array*), que introdujo la programación de dispositivos bajo una lógica que puede ser configurada en cualquier momento y ofreciendo funcionalidades acordes a la necesidad (Ley et al., 2009).

Por otro lado, se destaca el desarrollo de sistemas de comunicaciones como la *radio definida por software* (en inglés, SDR, (por las iniciales de *Software Defined Radio*), que integra funciones de *software* de la electrónica análoga, y

que permitió modificar o sustituir programas e, igualmente, adaptarse a las necesidades particulares de diseño requeridas (Manulis et al., 2020). Todos estos avances en la informática hacen que el *software* y su funcionalidad sea del todo pertinentes a las tecnologías satelitales, al no contar con masa, ni espacio ni demanda de energía, y porque permite su reprogramación desde la Tierra. Sin embargo, también presenta algunas dificultades: el *software* es inmaterial, complejo, vulnerable al error y de costoso desarrollo. A pesar de esto, es el núcleo de una misión espacial, que determina el fracaso o el éxito del proyecto (Ley et al., 2009).

Lo anteriormente mencionado, debe ser operado desde un centro de control; en muchos casos, desde lugares remotos, con una infraestructura provista de sistemas de recepción de señales electromagnéticas, informáticos y redes de comunicación, y donde la información se almacena y se transfiere a través de protocolos compatibles con FTP (TCP/IP). Por lo general, los equipos y los componentes se encuentran estandarizados bajo medidas de protección en materia de ciberseguridad, a fin de comprometer la confidencialidad, la disponibilidad o la integridad (Ley et al., 2009).

Marco regulatorio los dominios espacial y ciberespacial

Tomando en cuenta la estrecha interrelación entre estos dos dominios, es necesario precisar el ámbito regulatorio internacional que los circunscribe, por lo cual se resaltan cuatro marcos legales que deben ser tenidos en cuenta para la identificación de las amenazas cibernéticas que comprometen los sistemas satelitales y sus comunicaciones, los cuales, a su vez, tienen numerosos aspectos de aplicación en común, y que, a su vez, permiten una complementariedad.

El primero de ellos, de acuerdo con Housen (2016), es el colectivo de seguridad desarrollado por la Carta de las Naciones Unidas (Organización de las Naciones Unidas (ONU, 2002), y compuesto por la Oficina de Asuntos del Espacio Ultraterrestre (en inglés, UNOOSA, por las iniciales de United Nations Office for Outer Space Affairs) y la Comisión sobre la Utilización del Espacio Ultraterrestre con fines Pacíficos (en inglés, COPUOS, por las iniciales de United Nations Committee on the Peaceful Uses of Outer Space). Dicho colectivo está enfocado en a la contribución del espacio al logro de los Objetivos de Desarrollo Sostenible (ODS) (Flórez, 2020). En este marco se presentan algunos vacíos respecto a los parámetros de aplicabilidad de la ley frente al uso de la fuerza cuando un Estado

es víctima de un ataque hostil a sus activos espaciales[2], de forma virtual o híbrida, y llevado a cabo a través del uso del espectro electromagnético, el cual, a su vez, es uno de los medios mencionados en varias de las definiciones del dominio ciberespacial, como, por ejemplo, la del Manual de Tallín.

En consecuencia con lo anterior, cabe citar los tratados relacionados con el espacio exterior, que iniciaron su desarrollo a comienzos de la década de 1950, y comprenden cinco convenios. En ellos se menciona la imposibilidad de que los Estados reclamen soberanía sobre posiciones en el espacio, la Luna o cualquiera de los planetas, aunque sí pueden hacerlo sobre los objetos espaciales que sean lanzados, y se establece responsabilidad por los daños ocasionados a estos por los desechos derivados. De manera similar al primer marco normativo, se plantea el interrogante de si el tipo de daño en su modalidad virtual puede ser interpretado como un causal de responsabilidad por daños a terceros (Housen, 2016).

En tercer lugar, se encuentra la normatividad relacionada con el régimen regulatorio de la Unión Internacional de Telecomunicaciones (en inglés, ITU, por las iniciales de International Telecommunication Union), y que ha sido establecida de manera muy explícita, de gran robustez y ampliamente aceptada para asignar espacios orbitales o espectros de radiofrecuencia, y para determinar el tiempo de vida útil de las plataformas, así como para facilitar la comunicación ininterrumpida de los sistemas satelitales, a través de una operación transparente que impida a un Estado afectar a otro. Dicha normatividad prohíbe taxativamente interferencias, al igual que transmisiones innecesarias, engañosas o sin identificación. Con respecto a las dos regulaciones mencionadas, esta última aborda específicamente la protección al principio de disponibilidad —y parcialmente, al de integridad— de las señales de radiocomunicación (Housen, 2016; Flórez, 2020; International Telecommunications Union, 2020).

Por último, en materia de regulación espacial, se encuentra la *libertad transfronteriza de información*, reconocida tanto por tratados internacionales como por el derecho consuetudinario, y amparada bajo la Declaración de los Derechos Humanos, según la cual, a su vez, cualquier individuo tiene derecho a la libre expresión y a la libre opinión, sin interferencias, para buscar, recibir

2 "Cualquier activo de identificación única creado por el hombre en el espacio o diseñado para ser lanzado al espacio, y que comprende una nave espacial como un satélite, una estación espacial, un módulo espacial, una cápsula espacial, un vehículo espacial o un vehículo de lanzamiento reutilizable. Una carga útil (ya sea de telecomunicaciones, navegación, observación, científica o de otro tipo). Parte de una nave espacial o carga útil" (Sundahl, 2013, p. 3).

e impartir información e ideas a través de cualquier medio, sin importar las fronteras (Housen, 2016). Por otro lado, en cuanto al dominio ciberespacial existe como referente normativo: el Convenio de Budapest, generado en 2011 en la región europea, y donde se han establecido herramientas jurídicas para "prevenir, investigar y judicializar actividades y conductas delictivas cometidas a sistemas informáticos" (FAC, 2015, p. 14), dividiendo los delitos informáticos en cuatro grandes grupos. El primero de ellos es el relacionado con actividades ilícitas en contra de la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos, acorde con el marco normativo que involucra a los sistemas espaciales; sin embargo, ello solo es aplicable para los Estados signatarios a la fecha, lo cual limita su alcance. Asimismo, cabe mencionar el Manual de Tallín: una iniciativa no gubernamental que define los fundamentos para el desarrollo de la ciberguerra y la relación entre delitos y ciberespacio; en sus apartes detalla que un ataque de interrupción o pérdida de control de un satélite militar para un Estado constituye una violación de su inmunidad soberana (Schmitt, 2017).

En el hemisferio occidental —de manera más precisa, el continente americano—, a través de la Resolución de la Asamblea General de la (OEA,) se ha desarrollado una estrategia con el propósito de generar y elevar la cultura de seguridad y contrarrestar las amenazas en el ciberespacio, mediante la creación de una red de equipos nacionales de respuesta, la inclusión de normas técnicas para un uso más seguro de internet y la promulgación de un marco jurídico para proteger a los usuarios y para una mejor cooperación en contra de la ciberdelincuencia (FAC, 2015). El aspecto normativo y regulatorio de dicha estrategia se abordará y se discutirá de manera detallada en el numeral 7.4 *Políticas de Seguridad y Defensa aplicables al Espacio y al Ciberespacio en el Estado colombiano*, al interior del Estado colombiano.

Características y actores de la ciberseguridad aplicada al dominio espacial

Habiéndose descrito el contexto histórico del dominio ciberespacial, su relación con las aplicaciones espaciales y el marco regulatorio que los relaciona, y tomando en cuenta el alcance global, la interconectividad, la virtualidad y la instantaneidad que también relacionan estos dos dominios (FAC, 2020a), es preciso detallar algunos aspectos sobre los cuales se fundamenta la ciberseguridad con énfasis en los sistemas espaciales.

En general, existen tres principios o atributos que se deben cumplir a fin de mantenerse protegidos los activos: la *confidencialidad*, que permite mantener el secreto o la reserva de la información; la *disponibilidad*, relacionada con el aseguramiento del acceso permanente a los servicios, y por último, la *integridad*, que propende por evitar la manipulación y la alteración de la información que comprometa la funcionalidad del sistema (Llongueras, 2011; FAC, 2015; Wang et al., 2016).

De cada uno de los mencionados elementos derivan amenazas que comprometen la seguridad de plataformas satelitales y estaciones terrenas, y que es preciso mitigar mediante la búsqueda de un nivel apropiado de protección y de competencia en la ciberseguridad o, dado el caso, responder frente a las amenazas o los ataques con el fin último de asegurar el normal desarrollo de las misiones o los servicios para los que fueron concebidos estos activos, y lo cual es función de la ciberdefensa (Becerra et al., 2019; FAC, 2020c).

En específico, de acuerdo con el Manual de Ciberseguridad y Ciberdefensa FAC (2015), y según Becerra et al. (2019), la *ciberseguridad* es comprendida como la serie de herramientas, estrategias, prácticas y tecnologías que, bajo una acertada administración del riesgo, contribuyen a proteger los activos informáticos y a sus usuarios en el ciberespacio. Aunque este manual no detalla políticas o medidas de protección relacionadas con el dominio espacial, sí considera una *estación terrena*, o en otras palabras, el segmento terrestre, como un elemento de la infraestructura crítica de la FAC. Por otro lado, el manual de Doctrina Básica de la FAC determina dentro de la función del dominio del aire, el espacio y el ciberespacio la misión de *contrapoder espacial*, el cual sustenta las operaciones que puedan contrarrestar las capacidades espaciales adversarias y, paralelamente, velar por la protección de los activos espaciales propios, y así garantizar el acceso autónomo y la operación permanente (FAC, 2020c).

Para poder cumplir con este rol institucional, la FAC cuenta con marcos normativos que protegen el acceso a la información: por ejemplo, la Norma Internacional ISO 27001 y las publicaciones especiales de la familia *NIST SP 800* (Bichler, 2015; Vera, 2016; National Institute of Standards and Technology, 2018a, 2018b, 2020). Asimismo, en el ámbito nacional se han desarrollado: la *Guía de Protección Específica para la Infraestructura Crítica Cibernética Nacional*; el *Plan Nacional de Protección y Defensa de la Infraestructura Crítica Cibernética Nacional*, y el *Plan Sectorial de protección y Defensa para la Infraestructura Crítica Cibernética del Sector Seguridad y Defensa-Sector TIC* (Comando Conjunto Cibernético, 2020).

Dichas estrategias normativas son implementadas con el fin de proteger los activos frente a los diversos actores que intervienen en el ciberespacio. Por eso, se detallará seguidamente la intervención de las partes involucradas, con el propósito de comprender su interacción.

De acuerdo con Tovar y Chávez (2017), es posible agrupar en el ciberespacio a los actores en tres categorías. Una de estas es el *gobierno*, que centra sus actividades en la ciberguerra, el ciberespionaje y las operaciones de influencia, mediante la activa aportación de los equipos de respuesta a incidentes de seguridad informática (CSIRT), de emergencias cibernéticas (CERT) y las demás instancias nacionales de las Fuerzas Militares (FF. MM.); por otro lado, se encuentran las organizaciones estructuradas y los individuos bajo las redes; estos últimos, a su vez, se disgregan en una larga lista de participantes: *hackers*, hacktivistas, terroristas, operadores *botnet*, *phishers* y *spammers*, entre otros (Centro Criptológico Nacional, 2020).

Estos últimos actores —en su mayoría, considerados atacantes— implican un desafío a la ciberseguridad y a los intereses que esta protege, dada su complejidad, pues poseen diferentes tipos de motivación, que varían desde el ámbito social, económico o político hasta el militar, y pueden ser financiados por Estados, servicios de inteligencia, grupos terroristas, extremistas políticos o ideológicos, la delincuencia organizada o, simplemente, por atacantes de bajo perfil que no son otra cosa sino individuos con altos conocimientos en tecnologías de la información (Instituto Español de Estudios Estratégicos [IEEE], 2010; Bejarano, 2011; Grisales, 2015; FAC, 2015; Livingstone & Lewis, 2016).

Toda esta gama de nuevos actores relevantes conduce a cerrar la brecha de poder entre actores estatales y no estatales, dado que el dominio ciberespacial está enmarcado en un mundo digital donde la información es el activo estratégico más importante, y esta es vulnerable a la libre manipulación en un entorno altamente dinámico, en el que los marcos legales existentes no logran abarcar en su totalidad el accionar delictivo (Tovar & Chávez, 2017; Becerra et al., 2019).

El ciberespacio: una herramienta esencial en el espacio, pero, a su vez, un desafío

Sistemas espaciales, seguridad, defensa e intereses nacionales

Habiendo analizado el entorno nacional e internacional relacionado con la interacción entre el dominio espacial y el ciberespacial, y todos sus elementos constitutivos, es pertinente examinar estas capacidades bajo el enfoque de la seguridad y defensa, así como su rol respecto a los intereses nacionales, para posteriormente identificar sus amenazas y sus vulnerabilidades, y evaluar sus riesgos. Ello, con el propósito de establecer lineamientos que contribuyan a la Estrategia de Seguridad Nacional enfocada en la protección del dominio espacial (Ballesteros, 2016).

El Artículo 2.º de la Constitución Nacional contempla los fines esenciales del Estado, para lo cual la Fuerza Pública se constituye en la herramienta que garantiza su protección frente a amenazas tanto internas como externas, a través de la Defensa Nacional y utilizando medidas como la disuasión, la coerción o la represión, con el propósito de mantener el estado de seguridad nacional deseado (FF. MM., 1996), y asegurar así que los intereses de la nación se encuentren libres de interferencias o perturbaciones; para eso, la Fuerza Pública desarrolla una política nacional, compuesta por objetivos nacionales, voluntad política y una hoja de ruta que determine el mecanismo del uso del poder nacional (Bejarano, 2011); este último, extendido a nuevos dominios, como lo son el ámbito espacial y el ciberespacial (FAC, 2020a).

En el plano internacional, como parte de la política nacional de algunos países, el espacio exterior ha sido una prioridad para su seguridad nacional desde 1950 (Fidler, 2018). Los beneficios obtenidos como resultado del desarrollo de programas espaciales con propósitos militares, políticos y científicos han permitido que dichas capacidades se conviertan en parte de sus intereses nacionales. Estos intereses son una herramienta fundamental para la materialización de los fines del Estado, y por lo tanto, dada su importancia, es necesario que se encuentren "arraigados en la conciencia de la población y sus dirigentes" (FF. MM., 1996, p. 22); además, de manera intrínseca, como aspiraciones nacionales. Por consiguiente, como primera medida, son esenciales su definición al más alto nivel y su prolongación en el largo plazo, para su consecución.

Actualmente, Colombia no cuenta con una definición explícita de estos intereses, pues, a pesar que en el Plan Nacional de Desarrollo 2018-2022 se ha propuesto en el pacto por la Legalidad, en su objetivo 6: *Capacidades de Defensa y Seguridad Nacional*, identificar los intereses nacionales, no se aprecian, a la fecha, avances a ese respecto.

De acuerdo con López (2002), el poder aeroespacial, a través del uso de una gran variedad de medios disponibles, entre los cuales se encuentran las plataformas satelitales, proveen a los responsables políticos y militares información esencial a todo nivel para la acertada toma de decisiones, sin embargo, para su implementación se requiere factores de desarrollo, apalancados en una industria espacial, procesos científicos y tecnológicos, infraestructura educacional, políticas, la difusión de los intereses nacionales aeroespaciales y finalmente la capacidad de utilizar el espacio en pro de estos intereses (Bergamaschi, 2013).

Para el caso colombiano, de acuerdo con el Plan Nacional de Desarrollo 2018-2022, se ha trazado como una meta la necesidad de impulsar la transformación digital en el marco de la Cuarta Revolución Industrial, mediante la implementación de una política nacional, con la cual se fortalezca el uso de sistemas satelitales para analizar la productividad de la tierra, fortalecer la conectividad de alta velocidad y los sistemas de navegación; aplicaciones que conforman "componentes claves del *Ecosistema Digital*" (DNP, 2019b, p. 727).

Teniendo como referencia el Instituto Español de Estudios Estratégicos (2010), el sector aeroespacial hace parte de uno de los doce sectores que componen las infraestructuras críticas, pues las aplicaciones espaciales proveen, sin duda, servicios esenciales, y su funcionamiento ininterrumpido resulta indispensable para el Estado. De acuerdo con dicho criterio, y de acuerdo con la revisión de literatura llevada a cabo, ha de considerarse este sector para el caso colombiano, igualmente, como parte de la infraestructura crítica (FAC, 2015; Livingstone & Lewis, 2016); asimismo, y visto lo anterior, se sustenta el profundo interés manifestado por el gobierno actual en fortalecer estas capacidades.

No obstante lo anterior, y pese a la importancia de los sistemas satelitales y los esfuerzos en materia de ciberseguridad a escala nacional e internacional, el sector espacial no ha sido una prioridad en el contexto gubernamental, ni en el privado, lo cual no garantiza su protección ni su integridad como parte de la infraestructura crítica a través de un proceso de identificación, priorización, catalogación, gestión y monitoreo (Housen, 2016; Fidler, 2018; Falco, 2020).

Evolución de las amenazas en el marco de la seguridad multidimensional

La Declaración sobre la Seguridad en las Américas, concebida en 2003 bajo un nuevo concepto de *inclusión de nuevas amenazas*, incorporó una amplia variedad de aspectos políticos, económicos, sociales, de salud y ambientales (Chillier & Freeman, 2005), justamente, cuando la nueva era espacial emergía en la escena internacional, como parte de la revolución tecnológica, y esto, a su vez, llevó a la aparición de nuevos retos y desafíos provenientes del dominio ciberespacial, donde la ciberseguridad no fue considerada debidamente (Falco, 2020).

Tanto las amenazas tradicionales como las nuevas, al igual que los desafíos a la seguridad, son el foco de cooperación y fortalecimiento de capacidades entre los Estados miembros; los ataques cibernéticos (Grisales, 2015), hace más de dos décadas, están dentro de las preocupaciones por atender en materia de seguridad, buscando la protección de las infraestructuras críticas (Blackwell, 2015). Sin embargo, la inclusión acelerada de sistemas espaciales y actores en el ciberespacio amplía las brechas en materia de protección, dado el incremento de vulnerabilidades en relación con las amenazas existentes.

La transversalidad del ciberespacio con otros ambientes —en el contexto actual de la globalización, la hiperconexión y la innovación tecnológica— conduce a un incremento en la incertidumbre de los escenarios, en razón de la complejidad de sus amenazas, por lo cual la cooperación del sector público y el privado para el fomento de la cultura, la conciencia y la capacitación profesional, a través de políticas y marcos legales, resulta indispensable para afrontar las nuevas amenazas emergentes (Banco Interamericano de Desarrollo [BID], 2020).

Lo anterior, concibiendo como una amenaza en el ciberespacio, o *ciberataque*, a toda "Fuente potencial de perjuicio, interna o externa, a algún activo de la organización que se materializa a través del ciberespacio" (Junta Interamericana de Defensa, 2020, p. 14). Este tipo de amenazas debe considerar un elemento técnico, humano y una motivación en los activos de la víctima con el fin de causar daños, y lograr su degradación.

Desde el punto de vista militar y económico, el ciberataque a un activo espacial es una alternativa llamativa, tomando en cuenta la cantidad de satélites orbitando la Tierra, sus aplicaciones, que tienen un alcance estratégico, y la dificultad para atribuirse los hechos (Fowler, 2016; Livingstone & Lewis, 2016). Por otro lado, es importante mencionar los desafíos relacionados con las cadenas de suministro de componentes en el ciclo de ingeniería de diseño satelital, donde

la competencia de la oferta de mercado obliga a reducir los costos por parte de proveedores y, en ocasiones, a incumplir los estándares mínimos vulnerando la protección de los futuros activos espaciales y facilitando el accionar de los ciberatacantes (Hamilton, 2020).

Por todo lo anterior, la identificación y la valoración de ciberamenazas que afectan los sistemas espaciales resulta primordial como base para la prevención, la detección, la respuesta y la contención de estas (IEEE, 2010). En ese orden de ideas, las ciberamenazas tienen determinadas características, que permiten establecer la conducta de quien las origina. En primer lugar, está la táctica, o el "qué", concerniente a la estrategia y las herramientas utilizadas para lograr el objetivo propuesto. También está la técnica, o el "cómo", consistente en el método empleado. Por último, está el procedimiento, o conjunto sistemático de tareas por seguir para materializar la amenaza (Lewis et al., 2016).

Para hacer un análisis de las amenazas desde diferentes perspectivas, se ha elaborado una clasificación de estas en dos categorías. La primera, en función del modo como las amenazas se materializan y ocasionan un daño (i.e. cinético, virtual o híbrido)). En segundo lugar, y siendo la tipología más característica, la concerniente a los atributos de la ciberseguridad (i.e. confidencialidad, disponibilidad e integridad). Asimismo, en esta última clasificación las amenazas están direccionadas, por lo general, a un segmento en específico (i.e. espacial, terrestre o usuario final), como también, a las aplicaciones espaciales que pueden ser afectadas (i.e. comunicaciones, navegación y sensoramiento remoto). Por lo anterior, se describirán seguidamente las amenazas más representativas y los impactos de las dos clasificaciones en mención.

Modos de materialización de las ciberamenazas

Las amenazas en relación con la modalidad en que se presentan son diferenciadas en tres tipos: *cinético*, *híbrido* y *virtual*. La primera de ellas, la de tipo cinético, corresponde a un ataque físico directo de un elemento espacial contra otro, de modo que se produce una colisión entre ellos; un incidente denominado *ataque antisatélite* (ASAT, por sus siglas en inglés), o de otra forma, como resultado de un impacto con desechos espaciales.

En este evento existe un satélite soportado por sensores de proximidad, y comandando por un atacante, con la información orbital necesaria para localizar a un satélite víctima y lograr su propósito (Housen, 2016). Aunque esta técnica es un caso muy poco frecuente, ya se encuentra documentado en al menos tres

ocasiones: en 2007 se reportó la destrucción, por parte de China, de un satélite meteorológico de su propiedad, que se encontraba ya fuera de servicio. De igual forma, en 2008 Estados Unidos realizó un ejercicio similar con uno de sus propios satélites de observación de radar, y que falló tras su lanzamiento. Asimismo, en 2019 la India efectuó una prueba exitosa, con un microsatélite en la órbita baja (Manulis et al., 2020).

En una segunda categoría, de acuerdo con Housen (2016), se encuentran los ataques de tipo híbrido, en el que, a través de la línea de vista de un satélite víctima, se causa un daño material mediante la emisión de radiación tipo láser o pulso electromagnético. Su nombre obedece a la combinación de un ataque físico y uno virtual, que busca producir daños irreparables a un activo en el espacio.

Por último, y practicada más a menudo, está la modalidad virtual, también más afín a los sistemas de ciberseguridad actuales, y la cual tiene el propósito de afectar la confidencialidad, la disponibilidad o la integridad del servicio, mediante un ataque a los sistemas informáticos a través de la manipulación del espectro electromagnético o de los sistemas de redes, para así afectar la operatividad o la pérdida del control. En esta modalidad se profundizará a continuación (Housen, 2016).

Las ciberamenazas relacionadas con la intrusión: confidencialidad

Con respecto al acceso no autorizado a las aplicaciones, los sistemas informáticos o la información satelital, se presenta como vector más común la *explotación de redes de sistemas informáticos* (CNE)), o técnica que usa la implantación de *software* malicioso, a través del cual se instalan *virus*[3], *troyanos*[4], *gusanos*[5] o *botnets*[6] dentro del *hardware*, buscando comprometer la privacidad de la comunicación entre el segmento de Tierra y el espacial (Javaid et al., 2012). Existen,

3 Programa diseñado para copiarse a sí mismo, con la intención de infectar otros programas u otros ficheros (Bejarano, 2011, p. 71).

4 Programa similar a un virus, pero que se diferencia de este en su forma de realizar las infecciones. Mientras que los virus intentan infectar a otros programas copiándose dentro de ellos, los gusanos realizan copias de sí mismos, infectan a otros computadores y se propagan automáticamente en una red, independientemente de la acción humana (Bejarano, 2011, p. 71).

5 Programa que no se replica ni hace copias de sí mismo. Su apariencia es la de un programa útil o inocente, pero en realidad tiene propósitos dañinos, como permitir intrusiones, borrar datos, etc. (Bejarano, 2011, p. 71).

6 Red formada por computadores virtualmente secuestrados o infectados (robots informáticos, o *bots*) que ejecutan tareas de manera autónoma y automática, sin el conocimiento ni el consentimiento de sus legítimos propietarios o usuarios (Junta Interamericana de Defensa, 2020, p. 109).

asimismo, técnicas como los *keyloggers*[7], que, a diferencia de los anteriores, representan un serio problema, en la medida en que no pueden ser detectados por antivirus, por lo cual pueden monitorear la pantalla, la gestión de archivos y el uso de programas del sistema informático afectado (Manesh & Kaabouch, 2019).

En cuanto a las técnicas más comunes de ataque, es necesario citar el *pishing*, que se constituye en la forma más común de intrusión a los sistemas de Defensa de la Fuerza Aérea de Estados Unidos (Bichler, 2015), la cual, a través de un correo electrónico suplantando una página web legítima asociada a una organización, permite propagar la amenaza a través de la red en otra técnica, conocida como *movimiento lateral*, con la que se accede a los activos y la información clave del sistema.

El *ransomware*, otra importante modalidad de ataque, consiste en el secuestro de la información, y durante los últimos diez años ha afectado un significativo número de infraestructuras críticas; los sistemas terrestres satelitales son igualmente vulnerables.

De manera similar, pueden presentarse ataques donde se obtiene el control total o parcial sobre una plataforma satelital o sobre su carga útil; una táctica más conocida como *hijacking*, y que se hace más crítica cuando se trata de constelaciones satelitales, por cuanto un ataque a una de sus plataformas puede pasar inadvertida para la víctima (Manulis et al., 2020). Entre los sucesos más conocidos de *hijacking* se encuentran los ataques a los satélites de comunicación de Intelsat para la transmisión de televisión, perpetrados en 2007 en Sri Lanka, y en 2013, en Estados Unidos (Housen, 2016). En un caso similar, Ucrania fue acusada por Rusia de intentar obtener el control de uno de sus satélites de comunicación, con el fin de producir un decaimiento orbital y, con ello, su inutilización (Livingstone & Lewis, 2016).

Otra actividad estrechamente relacionada con el ciberespionaje, y de gran preocupación para las grandes organizaciones, es la *Amenaza Persistente Avanzada* (en inglés, APT, por las iniciales de *Advanced Persistent Threat*), y consistente en la intrusión sistemática a la red y sus activos informáticos por parte del atacante, con el fin de mantenerse indetectable por el mayor tiempo posible extrayendo información. La National Aeronautics and Space Administration ((NASA)) , o Administración Nacional de Aeronáutica y el Espacio, es considerada

7 Programa diseñado para hacer un seguimiento y un registro de la información y de los comandos introducidos en el teclado de un computador, de manera oculta con respecto al usuario (Manesh & Kaabouch, 2019).

uno de los más rentables objetivos de este tipo de agresión en el ámbito espacial, dado el valor que representan el desarrollo tecnológico y el conocimiento, como resultado de las décadas de investigación y los recursos invertidos en sus actividades (Bichler, 2015; Calderón et al., 2018).

Por último, entre las amenazas relacionadas con la confidencialidad que intercepta las comunicaciones entre el segmento espacial-terrestre o espacial-usuario se encuentra el *eavesdropping*, catalogada como otra de las tácticas más relevantes de esta clase, y que, por lo general, se materializa cuando hay protocolos de encriptación débiles. Entre los casos documentados de ciberespionaje se encuentran los relacionados con el grupo ruso *Turla*, el cual ha explotado la identificación y la replicación de direcciones IP de sistemas informáticos de usuarios suscriptores de servicios de internet satelital; sobre todo, en el continente africano. Su detección se dificulta, debido a que el usuario original no experimenta afectaciones en el rendimiento del sistema (Leopold, 2015; Falco, 2020).

Las ciberamenazas y la disrupción al servicio: disponibilidad

Antes de abordar las amenazas relacionadas con la denegación del servicio, es preciso clarificar que puede haber interferencias de carácter involuntario, como resultado de una operación inapropiada o por una falla del sistema, una distorsión de las ondas de radio por diversas causas (e.g. efectos de la ionósfera, meteorológicos, *doppler* u ocasionados por la tropósfera), o por interferencia con otras ondas de radio de sistemas de comunicación legales, debido a la saturación del espectro electromagnético (Wang et al., 2016).

Frente a las interferencias de tipo intencional, de acuerdo con Wang et al. (2016), el *meaconing* y el *jamming* son las técnicas más características de ataque, y van dirigidas a los satélites de comunicación y tomando en cuenta las consecuencias que implican la interrupción de su operación y la imposibilidad de ejercer medios sancionatorios contra los infractores, dados los vacíos en torno a las ya descritas regulaciones internacionales en el marco regulatorio del dominio espacial.

El *meaconing* se constituye en una amenaza a los servicios de navegación satelital empleados por estaciones terrenas, barcos, sistemas balísticos inteligentes o aeronaves durante la transmisión y la recepción de las señales, en la medida en que las retrasa y las retransmite con mayor potencia y usando la frecuencia original, con lo que se interpretan ubicaciones imprecisas por parte de

los dispositivos a bordo, y son, por lo tanto, una preocupación para el sector del transporte aéreo y para el marítimo, dada la crítica importancia de obtener una localización precisa (Wang et al., 2016; Manesh & Kaabouch, 2019).

Por otra parte, la degradación y la interrupción de la conectividad del sistema a través de la interferencia de las ondas de radio se denomina *jamming*. En dicha práctica puede haber un bloqueo tanto de las comunicaciones terrestres como de la señal orbital de la plataforma satelital. Para materializar esta amenaza se emplean equipos que, sencillamente, transmiten de manera indistinta en múltiples frecuencias; otros dispositivos niegan al receptor la captura de la señal, a través de la transmisión en la misma frecuencia electromagnética; por último, los más especializados tienen la posibilidad de bloquear anchos de banda específicos (Livingstone & Lewis, 2016).

Las ciberamenazas asociadas a la alteración a la información: integridad

A diferencia de los ataques a la confidencialidad y la disponibilidad de los sistemas informáticos, comprometer la integridad implica modificar y alterar la información que está almacenada o que circula a través del ciberespacio y, por ende, a través del espectro electromagnético. Existe la posibilidad de que, a causa de los fenómenos naturales, como el magnetismo terrestre o la radiación cósmica, se presente una afectación a la integridad de la información; sin embargo, en la mayoría de los casos la alteración ocurre de manera intencional (Javaid et al., 2012).

El *spoofing* es considerada una de las técnicas usadas por los atacantes para afectar la integridad, y que, a diferencia del *jamming* —donde se presenta un bloqueo de la señal—, en esta técnica la señal es suplantada por otra, que bloquea o anula la señal legitima, como resultado de lo cual el receptor sigue operando servicios satelitales, pero ahora basados en información alterada (Livingstone & Lewis, 2016; McKenna et al., 2018).

Entre las aplicaciones satelitales que pueden sufrir una mayor afectación se encuentran las relacionadas con los servicios de navegación satelital, mediante la alteración de la señal de los Sistemas de Vigilancia Dependiente Automática[8] (en inglés,

8 El sistema de Vigilancia Dependiente Automática, o ADS-B, es un sistema que reemplaza la tecnología de radar con satélites, para determinar la ubicación de una aeronave. Utiliza señales de satélite para rastrear la posición tridimensional y la identificación de aeronaves, los vehículos u otros activos, de manera automática, porque transmite información periódicamente, sin la participación del piloto ni del operador (Federal Aviation Administration, 2021).

ADS-B, por las iniciales de Automatic Dependent Surveillance-Broadcast) ()en el sector del transporte aéreo comercial, o del Sistema de Identificación Automática[9] (en inglés, AIS, por las iniciales de Automatic Identification System) ()a bordo de buques; ambos por supuesto, son sistemas indispensables para el monitoreo del tráfico aéreo y para la navegación marítima. Para este último caso, se tiene registro del uso de dicha técnica por parte de los tripulantes de embarcaciones usadas en actividades ilegales transmitiendo información falsa y ocultando sus verdaderas intenciones (Livingstone & Lewis, 2016; Manesh & Kaabouch, 2019).

En relación con el *spoofing*, se considera que representa una mayor amenaza que una afectación a la disponibilidad del servicio, en comparación al *jamming* o el *meaconing*, pues una recepción de señal alterada con completo desconocimiento por parte del usuario, dada su mayor dificultad de detección, conlleva mayores peligros para la seguridad aérea o la marítima, para el tráfico legal y, por lo tanto, para la seguridad nacional (Falco, 2020).

Contribución de los elementos espaciales, e incidentes documentados

La afectación a los atributos de la ciberseguridad a causa de las amenazas analizadas en el acápite anterior debe complementarse mediante algunos aspectos relacionados con las aplicaciones y los segmentos satelitales. Para ello, se presentará una revisión estadística de los ataques efectuados a los sistemas satelitales.

La *economía global espacial* registró para 2020 utilidades por valor de 271 billones de dólares, donde el 45 % de la productividad correspondió a la oferta de servicios satelitales. La comercialización de equipos en tierra correspondió al 48 %; la industria de manufactura satelital, al 5 %, y el sector de lanzamiento, tan solo al 2 %. Sin duda, el sector de servicios y sus productos derivados representan la gran mayoría del mercado satelital, con una participación del 93 %. Frente a las aplicaciones satelitales, los satélites de comunicación abarcan el 56 % de las ganancias. El 36 % corresponde a los servicios y, finalmente, los sensores de observación terrestre contribuyen tan solo con el 1 % (US Satellite Industry Association, 2021).

9 El sistema de Vigilancia Dependiente Automática, o ADS-B, es un sistema que reemplaza la tecnología de radar con satélites, para determinar la ubicación de una aeronave. Utiliza señales de satélite para rastrear la posición tridimensional y la identificación de aeronaves, los vehículos u otros activos, de manera automática, porque transmite información periódicamente, sin la participación del piloto ni del operador (Federal Aviation Administration, 2021).

Aunque los ciberataques relacionados con la afectación a la confidencialidad son comunes a todas las aplicaciones espaciales, las cifras ya relacionadas y los estudios revisados en la presente investigación evidencian cómo la mayoría de las amenazas asociadas a la disponibilidad y la integridad del servicio están enfocadas en afectar a los satélites de comunicación y navegación, mediante técnicas como el *meaconing*, el *jamming* y el *spoofing*, tomando como referencia el considerable costo de un activo espacial de este tipo, las utilidades que genera y, por lo tanto, la motivación que un atacante tendría para afectar la funcionalidad del servicio. Lo anterior queda en evidencia dado el gran volumen de incidentes de relevancia mundial asociado a ese tipo de aplicaciones espaciales (Manulis et al., 2020).

En cuanto a la estadística de ciberataques documentados, y tomando como base una recopilación de incidentes obtenidos de fuentes académicas, noticias y reportes por Manulis et al. (2020), se registraron 131 ataques a sistemas espaciales, que datan desde 1977 hasta 2019, lapso a lo largo del cual se categorizaron la táctica o la técnica asociada a la amenaza, el segmento afectado, la víctima del ataque y su causa.

Aunque es posible identificar ciertas limitaciones en el presente estudio —asociadas a la exactitud de la información recopilada, a la omisión de reportes que, por seguridad nacional, no fueron reportados, y otros que nunca fueron identificados—, sí es posible obtener una muestra estadística, que describe de manera general el panorama y el comportamiento de las ciberamenazas frente a los sistemas espaciales.

Frente a la categorización de las amenazas, la *explotación de redes de sistemas informáticos* y el robo o la pérdida de información generaron el 60 % de los incidentes; todos ellos, concernientes al segmento terrestre. Con el 14 % y el 13 %, respectivamente, se presentaron ciberataques en las modalidades de *jamming* y *hijacking*. Asimismo, se presentaron otros tipos de casos, que comprendieron el 11 % restante, como, por ejemplo, pérdidas de control, *eavesdropping*, *spoofing*, *pishing*, ataques antisatélite y negaciones del servicio.

En cuanto al tipo de segmento objetivo del ataque, el 63 % de los casos correspondió al segmento terrestre; el 29 %, al enlace de comunicaciones, y el 6 %, al segmento espacial. El 2 % restante se quedó sin clasificar en el estudio. Con respecto a la naturaleza de la víctima, el 70 % de los incidentes fueron contra el sector estatal; el 21 %, contra el sector industrial, y el 8 %, en igual proporción, en contra tanto del campo civil como del militar. En lo referente a la causa del ataque, las razones políticas y el espionaje de Estado contribuyen en el 15 % de las agresiones,

seguidas de varias causas que, individualmente, no superan el 3 %, como el espionaje corporativo, la fuga de datos, los mensajes de advertencia, la investigación científica, motivos personales y causas accidentales, entre otras (Manulis et al., 2020).

Vulnerabilidades satelitales

La gestión del riesgo es un proceso sistemático que requiere la identificación de potenciales tácticas y técnicas referentes a las amenazas, así como de las vulnerabilidades asociadas a los sistemas espaciales. Esta última característica es definida como la debilidad que puede comprometer los atributos de la ciberseguridad en sus sistemas informáticos, al ser explotada por un atacante, por lo cual, su revisión resulta de sumo interés en la descripción del panorama general que concierne a la afectación de los sistemas espaciales (OTAN, 2019).

El gradual aumento de lanzamientos al espacio y de la puesta en órbita de satélites —de tamaño cada vez menor— es proporcional a la aparición de nuevas vulnerabilidades, lo que constituye un reto a la ciberseguridad, dada la acelerada interconectividad de redes, la alta competitividad de las compañías satelitales emergentes que omiten controles de seguridad en sus sistemas y la falta de requisitos específicos de ciberseguridad para los activos espaciales, que requieren un grado considerable de autocontrol por parte de las organizaciones (Falco, 2019; Livingstone & Lewis, 2016), y que, junto con la desestimación de habilidades en un atacante, con limitada inversión, pueden afectar aplicaciones satelitales, con graves consecuencias. Bajo las consideraciones expuestas, es posible categorizar las vulnerabilidades en relación con el *software*, el *hardware* y el factor humano, para lo cual en el presente estudio solo se describirán, a continuación, las dos primeras clasificaciones (Hutchins, 2016).

El *software* utilizado en las aplicaciones satelitales presenta vulnerabilidades muy similares a las de los sistemas informáticos tradicionales (Hutchins, 2016), y comparado con las otras dos categorías en mención, tiene la posibilidad de ser modificado, actualizado o alterado de manera remota, situación que no ocurre con el *hardware* ni con el *firmware*[10] (Livingstone & Lewis, 2016). Por lo anterior,

10 El *firmware* es un tipo de *software* integrado directamente en una pieza de *hardware*. Funciona sin requerir una interfaz de programación de aplicaciones, ni un sistema operativo ni controladores del dispositivo, lo que proporciona las instrucciones y la guía necesarias para que el dispositivo se comunique con otros dispositivos o haga un conjunto de tareas y funciones básicas, según lo previsto (National Institute of Standards and Technology, 2020).

se facilita el acceso no autorizado a los sistemas y las redes mediante *puertas traseras*, como resultado de protocolos débiles de autenticación, falencias en el desarrollo del código o el uso de fuentes de dudosa procedencia (Lane et al., 2017).

El medio más común de ataque es a través de páginas web, donde se encuentran vulnerabilidades críticas en el mismo diseño de internet, tales como la facilidad para obtener una ubicación a través del sistema de direcciones, la carencia de codificación, la descentralización del sistema y la capacidad para difundir código malicioso (Vargas, 2014). Sumado a esto, la industria satelital se ha encaminado al uso de componentes existentes en el mercado, con capacidad para utilizar protocolos de internet y de la Red de Área Amplia (en inglés, WAN, por las iniciales de *Wide Area Network*), para incorporarlos a los sistemas satelitales, que, junto a una configuración particular, protocolos especializados y un presupuesto limitado, conduce a mayores desafíos a la ciberseguridad (Vera, 2016).

Los grandes avances de la computación en la nube proveen a los servicios del segmento de tierra una gran capacidad. Esta tecnología es parte de la infraestructura de un gran número de servicios satelitales —en su mayoría, de sensoramiento remoto—. Sus ventajas son atractivas: bajo costo, flexibilidad, redundancia e independencia, todo lo cual elimina las restricciones propias de permanecer en unas instalaciones para acceder a los servicios; requiere, por otra parte, una alta velocidad de conexión a internet (Barleta et al., 2020). Sin embargo, los proveedores de servicio en la nube carecen de mecanismos adecuados para garantizar una seguridad informática auditable y certificable, y ello impide asegurar una completa privacidad de las aplicaciones y de la información que es procesada (Manulis et al., 2020).

Con respecto a la categoría de vulnerabilidades asociada al *hardware*, cabe resaltar algunos inconvenientes que generan el diseño y la manufactura de plataformas satelitales con la incorporación de *componentes tomados del estante*, pues los estándares de ciberseguridad y el costo que ello implica para su implementación están en contraposición de la maximización de las utilidades en la industria satelital (Lane et al., 2017).

De acuerdo con Fowler (2016), para el caso del segmento espacial, el componente físico más vulnerable son las antenas de comunicación, por cuanto estas no tienen la capacidad para determinar el origen de una frecuencia sin la asistencia de otros dispositivos. Desde la década de 1990, los atacantes han usado

esta técnica para interrumpir la señal y, en algunos casos, impartir comandos degradando su control. Este último es uno de los mayores peligros que enfrentan los satélites. Sumado a lo anterior, la mayoría de los protocolos de comunicación están diseñados para ser paquetes de datos de tamaño reducido, para así optimizar la demanda de energía y la velocidad de transferencia de la información, teniendo como premisa que un consumo de recursos puede llevar a un satélite a desactivar los controles de seguridad. Actualmente, no existe consenso en la industria espacial sobre las mejores prácticas en cuanto a las comunicaciones y los protocolos de autenticación segura (Manulis et al., 2020).

El segmento terrestre se constituye, sin duda, en el medio más vulnerable para un ciberataque, en razón de que provee los equipos y el *software* para tomar de manera legítima el control del segmento espacial (Bichler, 2015). Asimismo, este presenta vulnerabilidades similares a las de los sistemas informáticos de otros sectores industriales, pero con la particularidad de que algunos activos en el espacio y sus estaciones terrenas se componen de *hardware* y *software* de décadas anteriores, y que no poseen los estándares de ciberseguridad actuales (Hutchins, 2016), y por otro lado, el uso de equipos de radiofrecuencia y equipos de prueba, todo lo cual hace más críticas las vulnerabilidades (Vera, 2016).

Por otro lado, en cuanto al segmento de red, es fácil obtener información relativa al propósito y las características de un determinado satélite o de una constelación, y ello los hace vulnerables a ciberamenazas. Los datos referentes al consumo de energía y órbita mediante sensores, así como la transmisión de señales de la plataforma bajo ciertas condiciones y regiones del mundo, pueden determinar los objetivos de la misión. Asimismo, el registro de frecuencias y espacios orbitales ante en la Unión Internacional de Telecomunicaciones (UIT) —una organización de las Naciones Unidas que tiene jurisdicción sobre las actividades espaciales mundiales—, como también, ante las entidades nacionales que regulan el uso del espectro en el ámbito nacional, obliga a publicar la información de radiofrecuencia, y así brinda una amplia oportunidad a los actores interesados para identificar y registrar las señales de radiofrecuencia, con el propósito —a veces, malintencionado— de desarrollar ingeniería inversa para afectar la integridad o la disponibilidad de los activos espaciales; un desafío que no desaparecerá en el corto plazo (Manulis et al., 2020).

Otro aspecto crítico asociado al segmento red corresponde a la autenticación de la señal de comunicación, la cual emplea, generalmente, mecanismos de firma digital, consistentes en la emisión de una señal adjunta al mensaje enviado

por medio del espectro electromagnético; sirve como método de validación de autenticidad. Este proceso se realiza a través de componentes de radio definida por *software* (en inglés, SDR[11], (por las iniciales de *Software Defined Radio*), lo cual ofrece ventajas por su bajo costo, en comparación con el uso de *hardware* de propósito específico; pero debido a que emplean protocolos independientes del sistema, dichos componentes también introducen vulnerabilidades asociadas al *software* (Manulis et al., 2020).

Finalmente, cabe destacar la recopilación de vulnerabilidades que se hacen evidentes en un estudio realizado por Santamarta (2014), en el cual se hizo una evaluación de vulnerabilidades a diez importantes estaciones de servicios satelitales de comunicación, entre las cuales se encontraban Inmarsat-C, VSAT, BGA, FB y Classic Aero Service, entre otras, y donde se hallaron mecanismos débiles para el restablecimiento de contraseñas, puertas traseras, credenciales de acceso inmersas en código fuente y protocolos inseguros. Con estos hallazgos se definieron algunos escenarios de ataque a través de los cuales se pueden explotar las vulnerabilidades en mención, y así causar afectaciones a los servicios satelitales. Cabe concluir que incluso las grandes plataformas se encuentran expuestas a múltiples ciberamenazas.

Panorama espacial colombiano: retos, tendencias, avances y estrategias

Panorama satelital colombiano

Colombia, con sus características distintivas, y comparada con el resto de países de la región, es un lugar de contrastes. Su variedad de ecosistemas, su biodiversidad, su accesibilidad a dos océanos y su extensa línea de costa proveen un gran potencial de desarrollo económico y social; por otro lado, la cordillera de los Andes y la Amazonía, no obstante poseer una enorme riqueza de recursos, dificultan el acceso al interior del país, y con esto, a la incorporación de las tecnologías disruptivas y el desarrollo.

Estas particularidades conducen a la apremiante necesidad de explotación de diversas capacidades satelitales (Latam Satelital, 2016), considerando

11 Sistema de radiocomunicaciones que integra funciones de *software* de la electrónica análoga, y que permite modificar o sustituir programas e, igualmente, adaptarse a las necesidades particulares de diseño requeridas (Manulis et al., 2020).

los compromisos adquiridos por Colombia para 2030, y en nombre de los cuales el país ha participado activamente en la definición de los ODS (2015-2030), el Marco Sendai para la Reducción del Riesgo de Desastres (2015-2030) y el Acuerdo de París (CONPES, 2020a); todos ellos, afines a la explotación del espacio. Desafortunadamente, a pesar de algunos esfuerzos efectuados, aún no se han materializado iniciativas previas que permitan el desarrollo espacial a gran escala, tomando en cuenta los beneficios asociados a la potencial capacidad de tecnificación en un lapso corto, para permitir a largo plazo una mayor rentabilidad, una mayor diversificación y una mayor competitividad (Flórez, 2020).

Para dar dinamismo a esta problemática, se desarrolló el documento CONPES 3983 *Política de Desarrollo Espacial* (2020a), como un mecanismo de política pública, y que tiene el propósito de desarrollar condiciones habilitantes para el aprovechamiento de los sistemas espaciales. En su parte introductoria, dicho instrumento identifica falencias que residen, mayoritariamente, en factores estatales: falta de visión estratégica y de claridad en los intereses nacionales a largo plazo; debilidad institucional para articular medios, modos y partes interesadas hacia un fin común, y la ausencia, por último, de conocimiento por parte del sector que vislumbre oportunidades y facilite la entrada de inversión privada; esto último, teniendo como premisa, de acuerdo con Flórez (2020), que los proyectos espaciales producen, por lo general, una tasa de retorno en un tiempo mayor que doce años.

A pesar del incipiente acceso a los sistemas espaciales por parte de Colombia, en el que la contratación de aplicaciones utilizadas es realizada a terceros, durante 2018 se adquirieron servicios por un valor de 282 millones de dólares, de los cuales el 55 % correspondió a servicios de comunicación; el 44 %, a sistemas de navegación, y tan solo el 1 %, para observación de la Tierra (CONPES, 2020a).

Actualmente, la oferta nacional en el sector de las comunicaciones cuenta con once operadores satelitales que prestan el servicio de internet. En este sentido, el mercado corporativo cuenta con 8.692 accesos, y acumula, por tanto, el 91 % del total de accesos contratados, mientras que los accesos restantes corresponden a la categoría residencial, con el 9 % (DNP, 2019a). Por otro lado, la demanda satelital se encuentra compuesta, mayoritariamente, por entidades del Gobierno nacional: el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), para el programa Kioscos Vive Digital; el Ministerio de Educación Nacional (MEN), para la conectividad de centros educativos, y la Aeronáutica Civil, la Policía Nacional (PONAL), la FAC y el Ejército Nacional (EJC),

quienes utilizan esta rama de servicios e invierten anualmente cerca de 98 millones de dólares, correspondientes al 63 % del gasto total de este mercado; el 37 % restante, correspondiente a 57 millones de dólares, es utilizado por operadores privados de televisión, internet y telefonía (CONPES, 2020a).

La propuesta de adquisición de un satélite de comunicaciones en Colombia data de 1977. Para 2009, dicha iniciativa tuvo una apropiación de 250 millones de dólares, pero la evaluación de la propuesta declaró desierto el proceso; en segunda instancia, fracasó por diferencias entre los oferentes, y finalmente los recursos fueron destinados a la adecuación de la red de fibra óptica. Es importante tomar en cuenta que el uso de las tecnologías satelitales de comunicaciones —en especial, para el uso de internet— tiene el potencial de favorecer, considerablemente, al 89 % de los municipios del país, los cuales cuentan con una densidad poblacional menor de 200 habitantes por km2, lo cual, a su vez, corresponde al 40 % de la población total del país; asimismo, es la opción más viable, dadas las dificultades técnicas y los altos costos que implica la adecuación de las microondas o de la fibra óptica en las regiones más apartadas (Ministerio de las Tecnologías y la Comunicación [MinTIC], 2020).

Por tal motivo, y con el propósito de mejorar las condiciones de vida y la calidad educativa disminuyendo los costos de comunicación propios del acceso a internet, se emprendió, a partir de 2021, el proyecto Estratégico Nacional *Acceso Universal a las Tecnologías de la Información y las Comunicaciones en Zonas Rurales o Apartadas*, que busca garantizar un horizonte de ocho años de servicio, y que beneficie a 1.300.000 personas, y a un costo total de 2,1 billones de pesos (CONPES, 2020b).

En el campo de las tecnologías satelitales de navegación, y con base en los reportes mundiales del sector y del *Global Navigation Satellite System* (GNSS), el mercado de servicios satelitales de navegación se clasifica, principalmente, en tres áreas: servicios basados en localización (en inglés, LBS, por las iniciales de *Location Based Services*) —que son servicios aplicados a la agricultura de precisión—, y los servicios aplicados en vehículos o carreteras. Esta tipología permite identificar que el mercado de navegación satelital es dominado por los servicios masivos de LBS; los dispositivos asociados a dicho servicio son los teléfonos inteligentes y las tabletas, los cuales representan más del 90 % del total acumulado para 2017 a escala mundial (DNP, 2019a).

Para el caso colombiano, y teniendo como referencia las cifras estadísticas globales mencionadas, para 2016 el 73 % de los colombianos tenían acceso a un

teléfono inteligente, lo cual representó el 80 % de los servicios de navegación, y ello permite establecer un estimado de $312 millones de dólares, comprendido por el costo de los dispositivos GPS y los servicios de datos para aplicaciones que utilizan geolocalización. Cabe resaltar que el estimado de consumo mencionado, a pesar de su aportación en el mercado, no es tenido en cuenta en la participación de la tecnología satelital de navegación, por cuanto es considerado un servicio de valor agregado. Sin embargo, en lo referente al mercado satelital de navegación para 2017, el Instituto Geográfico Agustín Codazzi (IGAC), el Servicio Geológico Colombiano, las aplicaciones de agricultura de precisión y el sector vehículos y carreteras generan una demanda estimada de 312 millones de dólares, con una tendencia de crecimiento anual de, aproximadamente, el 27 % (DNP, 2019a).

En cuanto al uso de servicios satelitales de observación de la Tierra —un mercado mucho menor, en comparación con los dos anteriores—, existe una amplia gama de proveedores para el procesamiento de imágenes satelitales, comprendida por cuatro proveedores locales: Geospatial, Multiprocesos SIG S. A., Pro Cálculo y ESRI Colombia, que prestan servicios de procesamiento de las imágenes de las plataformas satelitales, entre las cuales, a su vez, se destacan WorldView-4, GeoEye-1, Airbus, Constelación Pléiades, Spot 6/7, y Kompsat-3 (DNP, 2019a).

En cuanto a la demanda satelital, el Instituto de Hidrología, Meteorología y Estudios Ambientales (IDEAM), el Servicio Geológico Colombiano (SGC), la Dirección General Marítima (DIMAR), la (FAC) y el (IGAC) dominaron el mercado de consumo, con el 87 % del gasto en 2017, equivalente a 1,46 millones de dólares (CONPES, 2020a). Además, la penetración de servicios tiene una estimación de crecimiento del 24 %, con una gran oferta de servicios satelitales de alta resolución y precios decrecientes.

Frente al uso de capacidades autónomas, como el diseño y el lanzamiento del satélite Libertad 1, de la Universidad Sergio Arboleda; la puesta en operación, en 2018, del satélite FACSAT-1 —con una vida útil de cinco años, aproximadamente—, y el futuro desarrollo del FACSAT-2, proyectado para su lanzamiento por la FAC (CONPES, 2020a), se aprecian tres iniciativas que estimulan el desarrollo del ámbito espacial en el país. Sumado a ello, se encuentra en proceso de construcción el Centro de Control y Desarrollo Espacial de la Fuerza Aérea Colombiana, que tiene como propósito ser el centro de monitoreo de las actuales y las futuras capacidades, acorde ello con el cumplimiento del plan estratégico

de la institución, y dentro de las cuales, para 2042 se tienen proyectados, entre otras iniciativas y atendiendo necesidades estratégicas en el país, el diseño, el lanzamiento y la operación de una constelación de satélites que brinden cobertura de comunicaciones y sensoramiento remoto (FAC, 2020c).

Tendencias globales en seguridad aplicable a los dominios espacial y ciberespacial

Dada la transversalidad y el complemento natural existentes entre los dominios espacial y ciberespacial, en este apartado se presentan las tendencias globales aplicables a la seguridad en ambos; aquí se conjugan aspectos de amplia importancia, que permiten identificar y proponer opciones para contener las amenazas generadoras de crisis, mitigar los riesgos generados por las amenazas propuestas a lo largo del presente capítulo y analizar las vulnerabilidades ocasionadas por las eventuales amenazas objeto de estudio, así como entender los desafíos más relevantes aplicables a los dominios espacial y ciberespacial.

En el marco de análisis referente al dominio espacial, y en el trabajo de investigación *Space, the Final Frontier for Cybersecurity?*, desarrollado por Livingstone y Lewis (2016), se presenta una interesante hoja de ruta aplicable a los satélites, las tendencias futuras en el uso del espacio para el periodo 2020-2035. De acuerdo con Livingstone y Lewis (2016) se consideran cuatro grandes áreas que presentan oportunidades de desarrollo con la decisiva participación de la industria espacial y los innumerables actores del orden político, económico, sicosocial y militar comprometidos con este importante dominio: "New Space; Satellite Communication; Earth observation; and Position, Navigationa and Timing" (Livingstone & Lewis, 2016, pp. 11-12)

Lo anterior permite apreciar los planteamientos de Livingstone y Lewis (2016), quienes recalcan la importancia que reviste el acertado empleo de las constelaciones de satélites, en las que los vehículos se comunican entre sí de forma autónoma; el empleo de sistemas de retransmisión de datos para reducir la demora en la entrega de los mismos; donde hay servicios de internet basados en satélites que demandan una cobertura global, y con el desarrollo de cadenas de suministro (que generan producción de bienes y prestación de servicios habilitados y aplicables para el espacio) por parte de entidades con enfoque y proyección multinacionales.

Como complemento de las tendencias y las condiciones descritas (Livingstone & Lewis, 2016), se considera que el ritmo del cambio en la tecnología

espacial y las fuerzas del mercado no reguladas permitirán el desarrollo de las ofertas espaciales.

El dominio del espacio, incluyendo sus elementos terrestres, estará permanentemente integrado en la infraestructura global, lo cual significa que el espacio ahora debe considerarse, inevitablemente, un dominio en constante expansión y cambio, donde las aplicaciones de mercado se desarrollan constantemente, a un ritmo que los gobiernos no pueden controlar (p. 12).

El portal *Actualidad Aeroespacial (2021)*, de cara al desarrollo de las operaciones de transporte en el espacio, se presenta cómo *La Nasa y SpaceX firman un acuerdo conjunto de seguridad de vuelos espaciales*, con base en el intercambio de información, y para mejorar los niveles de seguridad espacial: "Dado que las empresas comerciales lanzan cada vez más satélites, es fundamental que aumentemos las comunicaciones, intercambiemos datos y establezcamos las mejores prácticas para garantizar que todos mantengamos un entorno espacial seguro".

Respecto a las tendencias de carácter cibernético, en el documento *Ciberamenazas y Cibertendencias CCN-CERT IA -13/19*, el Gobierno de España, a través del Centro Criptológico Nacional (2020), presenta la percepción de ciberincidentes observados para el periodo 2018, sobre los agentes generadores de amenazas, las vulnerabilidades observadas, los métodos y los objetivos de ataque, así como las medidas adoptadas para identificar y prevenir los riesgos en el ciberespacio; a raíz de ellos, se establecieron las tendencias más relevantes en el marco del dominio ciberespacial: aumento de ciberataques patrocinados por los Estados; ataques a la cadena de suministros; la nube como objetivo; la sofisticación del código dañino; ciberataques dirigidos a personas; el uso de dispositivos inteligentes en ciberataques; el incremento del *criptojacking*, y la inteligencia artificial (en inglés, AI, por las iniciales de *Artificial Intelligence*) como herramienta en los ciberataques, así como la adopción y la transición a la red 5G como herramienta que ampliará la superficie de ataque.

Además de lo anterior, en el documento *Ciberamenazas y Cibertendencias CCN-CERT IA -13/20*, el Centro Criptológico Nacional (2020) hace referencia a la condición generada por la pandemia del Covid-19, pues, desde el punto de vista de la ciberseguridad y su relación con el teletrabajo, se plantea que "se han propiciado un enorme despliegue de entornos tecnológicos de teletrabajo para salvaguardar la continuidad de actividades y negocios […] incorporando numerosas deficiencias de seguridad" (p. 36). En términos generales, y a modo de

visualización, se prevén a partir de 2020: incremento de los ataques, y vulnerabilidades relacionadas con redes domésticas o dispositivos personales; incremento del ciberespionaje; que los actores patrocinados por los Estados dispondrán de nuevas vías de entrada a su objetivos; ataques a farmacéuticas y a laboratorios dedicados a investigar el Covid-19; incremento en los casos de afectación a sistemas industriales; aumento en el número de ataques en lo relacionado con dispositivos y sistemas del (IoT), y ataques a servicios en la nube.

Por lo anterior, los riesgos generados por las múltiples amenazas abordadas (periodo 2018-2020) en las órbitas global y regional, así como en el interior del Estado colombiano, impactan, sin duda, el logro de los objetivos y los intereses nacionales; tal condición invita a los gobiernos a reflexionar sobre el incremento de la actividad legislativa y regulatoria, y a hacerlo de manera decidida y contundente, en el marco de la seguridad nacional; todo ello, a su vez, en el marco de la cooperación internacional, que resulta imprescindible.

Avances para la detección y la contención de las ciberamenazas

Con el apoyo de la (OEA) y del Centro Global de Capacidad en Seguridad Cibernética (GCSCC), de la Universidad de Oxford, el Banco Interamericano de Desarrollo (BID) presentó el *Reporte de Ciberseguridad aplicable a los riesgos, avances y el camino a seguir en América Latina y el Caribe (2020))*: un documento donde se evidencia con claridad la intención de hacer el análisis aplicable al *Modelo de Madurez de la Capacidad de Ciberseguridad*. En dicho reporte se presentan interesantes planteamientos: "Se trata de un modelo que busca ofrecer una evaluación del nivel de madurez de las capacidades de ciberseguridad de un país, asignándole una etapa específica que corresponde a su grado de logro en materia de ciberseguridad" (p. 42).

Lo anterior se hace llevando un proceso lógico y secuencial formulado en cinco etapas: inicial, formativa, consolidada, estratégica y dinámica. Asimismo, la evaluación de los niveles de madurez se divide en cinco dimensiones: 1) política y estrategia de ciberseguridad; 2) cultura cibernética y sociedad; 3) educación, capacitación y habilidades en ciberseguridad; 4) marcos legales y regulatorios, y 5) estándares, organizaciones y tecnologías. Estos se subdividen, a su vez, en un conjunto de factores que describen y definen lo que significa poseer capacidad de seguridad cibernética en cada factor, e indican cómo mejorar la madurez (BID, 2020, p. 43).

Respecto al estudio realizado, el BID (2020) aclara que "los datos primarios utilizados en este reporte se recopilaron mediante un instrumento en línea que se distribuyó a todos los Estados Miembros de la OEA […] en base a los datos validados a diciembre de 2019" (p. 43); asimismo, establece los siguientes factores, al igual que las correspondientes dimensiones abordadas:

> - *Dimensión 1*. Política y Estrategia de Ciberseguridad (Diseño de estrategia y resiliencia de ciberseguridad): D1.1. Estrategia Nacional de Ciberseguridad; D1.2. Respuesta a Incidentes; D1.3. Protección de Infraestructura Crítica; D1.4. Gestión de Crisis; D1.5. Defensa Cibernética; y D1.6. Redundancia de Comunicaciones.
>
> - *Dimensión 2*. Cultura Cibernética y Sociedad (Fomentar una cultura de ciberseguridad responsable en la sociedad): D2.1. Mentalidad de Ciberseguridad; D2.2. Confianza y Seguridad en Internet; D2.3. Comprensión del Usuario de la Protección de Información Personal en Línea; D2.4. Mecanismos de Presentación de Informes; y D2.5. Medios y Redes Sociales.
>
> - *Dimensión 3*. Educación, Capacitación y Habilidades en Ciberseguridad (Desarrollo del conocimiento de ciberseguridad): D3.1. Sensibilización; D3.2. Marco para la Educación; y D3.3. Marco para la Formación Profesional.
>
> - *Dimensión 4*. Marcos Legales y Regulatorios (Creación de marcos legales y regulatorios efectivos): D4.1. Marcos Legales; D4.2. Sistema de Justicia Penal; y D4.3. Marcos de Cooperación Formal e Informal para Combatir el Delito Cibernético.
>
> - *Dimensión 5*. Estándares, Organizaciones y Tecnologías (Control de riesgos a través de estándares, organizaciones y tecnologías): D5.1. Adhesión a los Estándares; D5.2. Resiliencia de Infraestructura de Internet; D5.3. Calidad del *Software*; D5.4. Controles Técnicos de Seguridad; D5.5. Controles Criptográficos; D5.6. Mercado de Ciberseguridad; y D5.7. Divulgación Responsable.

Tal como se presentará en el numeral 7.4 *Políticas de Seguridad y Defensa aplicables al Espacio y al Ciberespacio en el Estado colombiano*, este último busca fortalecer de manera progresiva las políticas en materia de seguridad cibernética, las cuales son plasmadas en los respectivos documentos CONPES 3701 de 2011 *Lineamientos de política para la Ciberseguridad y Ciberdefensa*, y en el CONPES 3854 de 2016 *Política de Seguridad Digital*, con el propósito de responder y contener las amenazas observadas en el dominio ciberespacial dando

la responsabilidad de *coordinador general de Seguridad Digital del Estado* a la Presidencia de la República.

Adicionalmente, se creó el Comité de Seguridad Digital, para tratar temas intersectoriales en materia de seguridad digital, tales como: política y normatividad para la seguridad digital, la protección y la defensa de la infraestructura crítica cibernética nacional; gestión de riesgos de seguridad digital, crisis y seguimiento a amenazas cibernéticas; protección de datos personales; asuntos internacionales de seguridad digital, y comunicaciones estratégicas para la seguridad digital.

Como complemento de lo anterior, el Ministerio de Tecnologías y Comunicaciones (MinTIC) cuenta con un modelo de seguridad y privacidad, cuyo propósito es garantizar la gestión y la implementación de buenas prácticas y estándares que permitan proteger los activos críticos de información y la infraestructura tecnológica, al igual que los sistemas de información y comunicaciones existentes en el territorio colombiano, incluida la campaña denominada *En TIC Confío*, que busca generar conciencia responsable de internet y las TIC (BID, 2020).

Políticas de seguridad y defensa aplicables al espacio y al ciberespacio en el Estado colombiano

Con el paso del tiempo, y dada la importancia de la temática tratada, aplicable a los dominios objeto de análisis, en el interior del Estado colombiano se ha formulado un amplio contenido normativo, así como políticas públicas, para atender las amenazas, los riesgos y los desafíos eventuales en los dominios espacial y ciberespacial, en concordancia con el marco regulatorio colombiano basado en la Constitución Política de Colombia en su artículo 217, la Ley 599 de 2000 *Código Penal colombiano* y la Ley 1273 de 2009 para la *protección de la información y de los datos*, así como las políticas en materia de ciberseguridad emitidas que se encuentran documentadas: el documento CONPES 3701 de 2011 *Lineamientos de política para la Ciberseguridad y Ciberdefensa*; el CONPES 3854 de 2016 *Política de Seguridad Digital*; el CONPES 3968 de 2019 *Declaración de importancia estratégica del proyecto de desarrollo, masificación y acceso a internet nacional*; el CONPES 3975 de 2019 *Política Nacional para la transformación digital e inteligencia artificial*, y el CONPES 3995 de 2020 *Política de Confianza y seguridad Digital* (Comando Conjunto Cibernético, 2021).

De manera complementaria, dentro del Ministerio de Defensa Nacional (MDN) se cuenta con un equipo nacional de respuestas a incidentes de seguridad

digital: el (Col-CERT), una dependencia que, de manera coordinada con el Centro Cibernético Policial (CCP) de la Policía Nacional, el Comando Conjunto Cibernético (CCOC) del Comando General de las Fuerzas Militares, la Fiscalía General de la Nación, el Equipo de Respuesta ante Emergencias Informáticas (CSIRT) del Gobierno nacional, y el Equipo de Respuesta ante Emergencias Informáticas (CSIRT) Financiero, tiene la misión de detectar incidentes que puedan convertirse en amenazas generadoras de crisis en el ámbito nacional; situaciones que, en caso de ser observadas, serán reportadas de inmediato a la Presidencia de la República, dada la condición dicha entidad de coordinador nacional de Seguridad Digital del Estado colombiano.

En adición a las políticas, las estrategias y la normatividad expuestas, se hace necesario indicar que Colombia, a través de su PONAL, forma parte tanto de la Organización Internacional de Policía Criminal (INTERPOL) como de la Oficina Europea de Policía (EUROPOL), condición que permite atender de manera efectiva las conductas y las actividades relativas al ciberdelito. De manera complementaria, se cuenta con la Ley 1928 de 2018 *por medio de la cual se aprueba el "Convenio sobre la Ciberdelincuencia" adoptado el 23 de noviembre de 2001 en Budapest (Hungría)*, con posterior adhesión por parte del Estado colombiano, el 16 de marzo de 2020.

En el ámbito doctrinal militar, se tienen referentes como el Manual de Seguridad y Defensa Nacional; el Manual de Doctrina Básica, Aérea, Espacial y Ciberespacial, y el Manual de Ciberseguridad y Ciberdefensa de la Fuerza Aérea Colombiana. Los mencionados documentos guardan relación y han servido de fundamento para la formulación de la Estrategia para el Desarrollo Aéreo y Espacial de la Fuerza Aérea Colombiana al año 2042 *Así se va a las Estrellas*, donde se plantea específicamente el liderazgo que debe ofrecer la institución militar aérea en los dominios aéreo, espacial y ciberespacial.

Todos estos regímenes normativos, sumados a los tratados internacionales aplicados al espacio presentan convergencias, pero afrontan retos ante la posibilidad de llegar a una solución legal a favor de los Estados que han sido víctimas de ataques cibernéticos perpetrados a sus sistemas espaciales, tomando en cuenta la constante actividad ilícita ejecutada tanto por países como por actores externos (Levi & Dekel, 2012; Leopold, 2015; The Union of Concerned Scientists, 2021).

Por lo tanto, varios autores (Llongueras, 2011; Housen, 2016) plantean la necesidad de implementar una ley internacional para su aplicación en el ciberespacio, tomando en cuenta la complejidad de los nuevos actores no estatales,

la naturaleza de dicho dominio y la dificultad de determinar su autoría ante un evento hostil perpetrado. Sin embargo, una acción altamente regulada liderada por instituciones gubernamentales podría ser inefectiva para permitir una pronta respuesta frente a las ciberamenazas dirigidas a los sistemas espaciales. Por lo anterior, resulta mas apropiado un enfoque ligeramente regulado que desarrolle estándares liderados por la industria, en estrecha colaboración con el sector estatal, facilitando la evaluación de riesgos, el intercambio de conocimiento e innovación, lo cual mejora la agilidad y respuesta efectiva frente a las amenazas (Livingstone & Lewis, 2016).

Asimismo, de acuerdo con Falco (2019), se carece de estándares y de regulaciones que restrinjan el uso de satélites, y de organismos gubernamentales que hagan cumplir los tratados, los estándares y las políticas en materia de ciberseguridad espacial. Sumado a lo anterior, pese al extenso contexto regulatorio colombiano en el campo de la ciberseguridad y la protección de la información digital, y como resultado de una revisión detallada en este proceso de investigación, no se tomaron en cuenta las amenazas propias del ámbito espacial ni los peligros que de ellas se derivan, ni se advierte sobre estas, lo cual puede explicarse en razón del incipiente desarrollo colombiano en materia espacial, como ya se ha discutido, pero que, en definitiva, requiere una concientización de la comunidad cibernética si se proyecta el desarrollo en materia satelital en el corto plazo para el país.

Gestión del riesgo cibernético en el espacio, y sus problemáticas

En el ámbito de la ciberseguridad, estimar la probabilidad de ocurrencia de una amenaza presenta grandes dificultades, tomando en cuenta el alto grado de incertidumbre de los escenarios y su predictibilidad, por lo cual la valoración del riesgo obedece a una perspectiva cualitativa basada en una correcta identificación de las amenazas, el nivel de exposición, sus impactos y el historial de incidentes, con el fin de determinar medidas y controles para mitigar el riesgo cibernético (Livingstone & Lewis, 2016; Becerra et al., 2019; OTAN, 2019).

Con el fin de establecer las medidas que sean del caso, es importante clarificar algunos aspectos que afectan la ciberseguridad en el espacio. El primer aspecto es que, sin duda alguna, las estaciones terrenas son el segmento más vulnerable a ataques, con el 60 % del total de incidentes reportados, y donde la *explotación de redes de sistemas informáticos* es la táctica más frecuente de

ataque. Como segunda medida, se ha documentado en numerosas ocasiones que las normativas de ciberseguridad aplicadas a sistemas satelitales carecen de una valoración y una mitigación permanentes, y de un monitoreo del riesgo a sus activos a lo largo del ciclo de vida de estos; en parte, porque persisten la incomprensión y la desinformación recíprocas entre la comunidad cibernética y la espacial (Bichler, 2015). Por último, hay serias limitaciones financieras para una mayor protección de los sistemas informáticos a través de protocolos y medidas más robustas (Livingstone & Lewis, 2016).

Adicionalmente, las medidas de protección implementadas tienden a converger, en la medida en que el grado interdependencia y de correspondencia se estrecha con el desarrollo tecnológico, pues internet requiere, en muchos casos, los servicios de comunicación satelital, y estos últimos son controlados por sistemas informáticos soportados en redes, en las cuales ninguna política de ciberseguridad está preparada para afrontar los futuros retos, lo cual incrementa los riesgos de seguridad (Fidler, 2018). A pesar de lo anterior, se mencionan algunas recomendaciones específicas para algunas de las amenazas abordadas a lo largo del capítulo.

En relación con las medidas para preservar los atributos de la ciberseguridad y hacer frente a la variedad de amenazas existentes, de manera previa a la implementación de controles técnicos, de acuerdo con Vera (2016), la serie de publicaciones especiales (SP) desarrolladas por el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, proporciona una gran variedad de guías y recursos que pueden aprovechar los operadores de estaciones terrenas —en especial, las de satélites pequeños—, y donde se establecen procedimientos para efectuar una efectiva gestión del riesgo para los sistemas informáticos, y medidas de contingencia, así como planes para afrontar casos de intrusión, detección y medidas de prevención para usuarios de los sectores público y privado, a fin de adoptar un enfoque de seguridad cibernética con base en estándares adoptados internacionalmente, pues, al carecer los sistemas espaciales de requerimientos de ciberseguridad específicos y de estándares obligatorios, necesitan un grado considerable de autorregulación que incremente su seguridad frente al ciberespacio (Falco, 2019).

Con respecto a las ciberamenazas como el *ransomware* o la *Amenaza Persistente Avanzada*, es muy importante fijar estrategias de respaldo de la información, así como el uso de autenticación multifactor, la implementación de sistemas de protección de punto final de próxima generación y la administración de cuentas con privilegios limitados (Crowdstrike, 2020).

Sumado a lo anterior, un control de gran importancia para los sistemas espaciales terrestres son las *pruebas de penetración*, que, a diferencia de una evaluación de riesgos o de una auditoría, consisten en evaluar amenazas específicas a través de la reproducción de un ataque, lo cual requiere un equipo certificado de expertos en ciberseguridad para ingresar al sistema (Bichler, 2015).

Por último, en lo referente a las amenazas asociadas al espectro electromagnético, se encuentran algunas recomendaciones, incluyendo: una adecuada asignación de la banda de radiocomunicaciones, a fin de eliminar interferencias intencionales como resultado de operar en la misma red de otros sistemas de comunicación; la identificación, la localización y la caracterización de emisión de señales en el rango de frecuencia asignada; técnicas de mitigación de interferencias, a través de la codificación del canal, y finalmente, implementar procedimientos de autenticación y encriptación (Wang et al., 2016).

Estrategias, recomendaciones y trabajos futuros para el fortalecimiento el ciclo de la ciberseguridad y la ciberdefensa frente a las ciberamenazas en el espacio en Colombia

En el contexto global, tomando en cuenta la proyección acelerada, año tras año, de nuevos sistemas satelitales, dispositivos y usuarios que aumentan el riesgo cibernético, y donde la inversión en ciberseguridad debe ser acorde y proporcional a la dependencia tecnológica y de internet (Bejarano, 2011), durante 2020 hubo pérdidas económicas por un valor estimado de 945 billones de dólares, en razón de los ciberataques ocurridos. Asimismo, se hizo una inversión en ciberseguridad por 145 billones de dólares; cuantías que, sumadas, superan el trillón de dólares, correspondiente al 1 % del producto mundial bruto, de lo cual es posible inferir los grandes retos que implican las amenazas asociadas al ciberespacio (Smith et al., 2020).

Por lo anterior, y tomando en consideración que la industria espacial ha generado un amplio espectro de aplicaciones tanto en el campo militar como en el civil, y que son de gran interés para más organizaciones y países para los cuales en el pasado eran capacidades inalcanzables, es el propósito de una nación emergente en el sector de las tecnologías espaciales —y específicamente, en materia de ciberseguridad— identificar su infraestructura crítica, los fines, los modos y los medios para protegerlos, así como identificar a los actores involucrados que amenazan el normal funcionamiento de sus capacidades (Llongueras, 2011).

Por consiguiente, es necesario reconocer, en primer lugar, el ámbito espacial como un proyecto de carácter estratégico nacional que apalanca la economía y que, por un lado, ofrece servicios tangibles en beneficio de la sociedad y, por otro, asegura la soberanía del territorio (Calderón et al., 2018), para así dar cumplimiento a los fines del Estado, en los que la FAC participa activamente como una entidad articuladora, "encargada de liderar el desarrollo espacial del sector defensa y del país en términos de operaciones espaciales, así como de impulsar la industria nacional espacial" (FAC, 2020b, p. 20).

Lo anterior, mediante el planteamiento de objetivos que faciliten cumplir los fines propuestos en materia de ciberseguridad, tales como proteger los activos satelitales de la nación, de manera que se cumpla la misión asignada, ejecutar operaciones a través del ciberespacio que ofrezcan una ventaja militar, defender la infraestructura crítica, y asegurar la confidencialidad de la información de toda actividad maliciosa de carácter cibernético, soportado ello en el crecimiento de la cooperación interagencial nacional e internacional, así como el de la industria (U. S. Department of Defense, 2018).

Frente a los modos de protección cibernética, de acuerdo con la OTAN (2019), las actividades ofensivas ofrecen una mejor relación costo-efectividad que las defensivas, desde la perspectiva tecnológica. Por tal motivo, debe considerarse por parte de la FAC, como preparación para un entorno de alta amenaza, la exploración de capacidades en las operaciones de *contrapoder espacial ofensivo*, enmarcadas en el Manual Operaciones Aéreas, Espaciales y Ciberespaciales, las cuales corresponden al rol de la ciberdefensa y pueden ser dirigidas contra las amenazas espaciales, a la infraestructura y a otros recursos del poder espacial del enemigo, a fin de reducir su capacidad y evitar "la transmisión de datos, atacando los sistemas en tierra empleando guerra electrónica, ataques ciber o ataques físicos" (FAC, 2020b, p. 20). Por otro lado, también se encuentran descritas las *operaciones defensivas*, que conciernen a la ciberseguridad, por medio de medidas activas para contrarrestar los medios usados por el adversario, y *pasivas*, para proteger los activos satelitales con el fin de evitar ciberataques a través de redes informáticas o del espectro electromagnético (FAC, 2020b).

Las capacidades mencionadas previamente, en un contexto de guerra frente a un adversario, presentan grandes ventajas, en razón de la autonomía con la que se pueden ejecutar, puesto que requieren menores coordinaciones interagenciales, y a que, a diferencia de los demás dominios del poder, no están sujetos a límites geográficos, por lo cual cabe considerarlas una herramienta

para contrarrestar de manera efectiva las amenazas, pero que, de manera interdependiente con los demás dominios, contribuyen a la seguridad y defensa de la nación (FAC, 2020b).

A fin de obtener la iniciativa en el país en materia de ciberseguridad y ciberdefensa, es conducente adquirir un liderazgo que permita generar conciencia, educación y entrenamiento frente a las vulnerabilidades de sistemas espaciales expuestos a ciberataques. Casos como el de China —donde el desarrollo de componentes tecnológicos de uso militar está subordinado a suplir de manera autónoma todas sus necesidades, así como la creación de institutos educativos, donde se realicen ejercicios de simulación de ciberataques y se integre el dominio ciberespacial dentro de ejercicios militares tradicionales (Llongueras, 2011)— es un clara muestra del fortalecimiento de la innovación y el impulso de la ciencia y la tecnología para desarrollar habilidades que permitan identificar las vulnerabilidades de *hardware* y de *software* (Becerra et al., 2019).

Paralelamente, el cultivo del capital humano especializado en ciencias de la computación para el desarrollo de *hardware*, *software* y análisis de datos constituye un aspecto crítico de la ciberseguridad y la ciberdefensa. Para ello, la inversión de recursos, la identificación del talento, la formación y el aseguramiento de su permanencia en el largo plazo en las organizaciones, mediante oportunidades de capacitación especializada, incentivos y compromisos de permanencia, deben ser premisas para alcanzar la protección y la resiliencia, tanto para el sector público como para el privado (U. S. Department of Defense, 2018).

Por todo lo anterior, espera un largo camino por recorrer, y se plantean trabajos futuros para fortalecer y garantizar de manera ininterrumpida las capacidades en el espacio. Frente a la ciberseguridad, se requiere la implementación de buenas prácticas para los activos satelitales existentes y futuros, donde se incorporen técnicas de vigilancia permanente de las amenazas, con sus tácticas y sus técnicas, así como el reconocimiento de las vulnerabilidades específicas de *hardware* y *software*; todo esto, para fortalecer la protección y la resiliencia cibernética sustentadas en el seguimiento de los estándares internacionales ya citados. En cuanto a las tecnologías disruptivas, la familiarización y la adopción de herramientas, componentes y equipos en el corto plazo relacionadas con la computación cuántica, tomando en cuenta las enormes capacidades de procesamiento y encriptación de la información que brindarán a futuro la superioridad en el ciberespacio y un entono seguro del espacio. Asimismo, la generación de redes de intercambio de experiencias como mecanismo de cooperación tanto

nacional como internacional, para acrecentar la conciencia y el conocimiento de las ciberamenazas asociadas al uso del espacio.

En relación con la ciberdefensa, en el marco doctrinario de la estructura misional de contrapoder espacial adoptada por la FAC en 2020 (FAC, 2020b) resulta de gran relevancia la inclusión de operaciones cibernéticas en el espacio dentro de los ejercicios militares y los juegos de guerra, pues resulta ser un mecanismo de aprendizaje y preparación para un escenario real, tomando en cuenta que, hoy día, el empleo de todos los dominios es un requisito para la defensa y seguridad contrarrestando efectivamente el accionar de grupos estatales o no estatales que pretendan desestabilizar la soberanía y la integridad de una país o de sus instituciones mediante la afectación de las infraestructuras críticas.

Por último, se propone, con los resultados expuestos en el presente trabajo de investigación, complementar y robustecer el Manual FAC-3.0-E "Operaciones Aéreas, Espaciales y Ciberespaciales"-MOAEC, tomando en cuenta la conceptualización descrita respecto al dominio espacial, el análisis hecho frente a la relación y la interdependencia estrechas con el dominio ciberespacial para una operación segura, la identificación de las amenazas y las vulnerabilidades que permiten elevar la conciencia sobre el riesgo del entorno espacial y las estrategias que pueden fortalecer la ejecución de operaciones de contrapoder espacial ofensivo y defensivo, soportadas en el dominio ciberespacial.

Conclusiones

Considerando las relaciones de interacción entre el dominio espacial y el ciberespacial, se puede determinar que los mencionados elementos han compartido marcos de tiempo y puntos de convergencia comunes durante sus etapas de desarrollo, los cuales fueron estrechándose a partir del surgimiento de la nueva era espacial, en 2003, a causa de la transformación tecnológica, de los componentes mecánicos a electrónicos, y la de estos, a su vez, a los sistemas asistidos por *software*, lo que les dio una alta complejidad y un gran nivel de sofisticación, y donde la innovación de los sistemas informáticos avanza a un ritmo mayor que la de los sistemas físicos.

A pesar de esto, el desarrollo de las tecnologías disruptivas en el contexto de la globalización de las cadenas de suministro, la hiperconectividad y la analítica de datos han acelerado el avance de la tecnología satelital de manera vertiginosa en los últimos tiempos, al facilitar el acceso a los servicios y las aplicaciones

ultraterrestres y lograr convertirse en factor dinamizador para el logro de los ODS; pero, por otro lado, el ciberespacio se ha trasformado en un medio en el que actores hostiles, mediante el empleo de ciberarmas, amenazan los sistemas asociados al uso pacífico del espacio exterior.

Por lo tanto, es conducente afirmar que existe una sólida dependencia del espacio sobre el ciberespacio, pues ambos elementos comparten aspectos afines en relación con principios, marcos regulatorios y partes interesadas; sin embargo, la ciberseguridad se ha vuelto un puente de conexión entre estos dominios, y un requisito esencial para garantizar un confiable y permanente acceso al espacio, situación que exige una identificación y una caracterización de las amenazas y las vulnerabilidades a las que se enfrentan los activos espaciales, a fin de mantener a cubierto de interferencias y perturbaciones los intereses nacionales o corporativos, según sea el caso.

Como resultado del proceso de investigación realizado, se establecieron dos tipos de clasificaciones para las ciberamenazas que afectan el dominio espacial, tras haberse hecho una revisión de casos documentados bajo el dominio público. La primera categoría hace referencia a la modalidad en que se materializa la amenaza, y donde los ataques de tipo virtual representan el mayor peligro en el espacio. En segundo lugar, se tipificó una categoría en función de los atributos de seguridad: confidencialidad, disponibilidad e integridad, donde la explotación de redes informáticas representa la mayor amenaza, el sector público es el más afectado, el segmento terrestre es el elemento más vulnerable y los satélites de servicios de comunicación son las más propensos a recibir ataques.

Se lidia con grandes desafíos en el sector espacial dentro del Estado colombiano y, en general, frente a la ciberseguridad, si se tiene en cuenta que el uso de los sistemas satelitales no es, hasta el momento, una prioridad para el país, a pesar de estar catalogados como parte de los intereses nacionales y de la infraestructura crítica en países desarrollados. Esto lleva a mantener un avance tecnológico y un desarrollo de políticas y normativas muy incipientes frente a las amenazas asociadas al espacio, que gradualmente presentan mayor tecnificación, y de las cuales debe existir una concientización por parte de los operadores y los usuarios de estas tecnologías en el territorio nacional.

Con respecto a la seguridad cibernética, resulta fundamental conocer las vulnerabilidades de los sistemas espaciales, que, como todo sistema informático, tienen falencias y errores en el diseño de su *software* y el de su *hardware*, así como en su operación y su interacción con otros segmentos satelitales y su

interfaz mediante el uso del espectro electromagnético, con el fin de hacer una apropiada gestión del riesgo.

Como complemento de lo anterior, y soportado en el análisis multidimensional para la identificación de las amenazas presentes en los dominios espacial y ciberespacial, las vulnerabilidades generadas por las amenazas observadas, la gestión del riesgo cibernético en Colombia y en el espacio, y las problemáticas por estos ocasionadas, partiendo desde un enfoque global y regional hasta abordar la condición que en dichos dominios enfrenta el Estado colombiano, permitieron tener claridad respecto a las tendencias globales que en seguridad aplican a los dominios espacial y ciberespacial, para, de esa manera, establecer las estrategias que han sido formuladas para la detección y la contención de las amenazas multidimensionales, tanto en el espacio como en el ciberespacio, en beneficio de la Nación colombiana.

Lo expuesto garantizó un acercamiento de tipo conceptual, de cara a las débiles políticas, las normatividad y la legislación escasas en el interior del Estado; limitaciones que afectan los intereses nacionales aplicables a estos dominios, y se convierte, por eso, en una oportunidad y, a la vez, en un referente de análisis para la toma de decisiones por parte del conductor político del Estado y del Alto Mando Militar colombiano, con miras a garantizar el uso efectivo de los activos y de las capacidades, así como el empleo del poder nacional en los dominios espacial y ciberespacial en el marco de la acción unificada (AU) del Estado. Tal condición se relaciona de manera directa con la importancia y la necesidad que reviste para la nación colombiana cumplir la *Estrategia para el Desarrollo Aéreo y Espacial de la Fuerza Aérea Colombiana al año 2042 "Así se va a las Estrellas"*, donde se plantea claramente el liderazgo que debe ofrecer la institución militar aérea en los dominios aéreo, espacial y ciberespacial.

Referencias

Actualidad Aeroespacial. (2021). *La Nasa y SpaceX firman un acuerdo conjunto de seguridad de vuelos espaciales*. https://n9.cl/7wiu0

Ballesteros, M. (2016). *En busca de una Estrategia de Seguridad Nacional*. Subdirección General de Publicaciones y Patrimonio Cultural.

Banco Interamericano de Desarrollo (BID). (2020). *Reporte Ciberseguridad 2020 riesgos avances y el camino a seguir en América Latina y el Caribe*. BID.

Barleta, E., Pérez, G., & Sánchez, R. (2020). *La revolución industrial 4.0 y el advenimiento de una logística 4.0*. CEPAL.

Becerra, J., Sánchez, M., Castañeda, C., Bohórquez, A., Páez, R., Baldomero, A., & León, I. (2019). *La Seguridad en el Ciberespacio, Un desafío para Colombia*. Escuela Superior De Guerra "General Rafael Reyes Prieto".

Bejarano, M. J. C. (2011). Alcance y ámbito de la seguridad nacional en el ciberespacio. *Cuadernos de Estrategia, 149*, 47-82.

Bergamaschi, J. L. M. (2013). *La defensa nacional: Relaciones vinculantes con la estrategia y el poder aeroespacial*.

Bichler, S. F. (2015). *Mitigating cyber security risk in satellite ground systems*. Air Command and Staff College Maxwell Air Force Base United States.

Blackwell, A. (2015). Seguridad multidimensional: Enfrentando nuevas amenazas. *Seguridad, Ciencia & Defensa, 1*(1), 6.

Calderón, C. Á., & Gutiérrez, C. C. (2019). El espacio exterior: una oportunidad infinita para Colombia. Bogotá DC: *Fuerza Aérea Colombiana*.

Calderón, C. E. Á., Valbuena, C. R. Á. M., Gutiérrez, C. C. G. C., & Zorrilla, C. M. F. (2019). El espacio exterior, escenario de competencia o cooperación en América del sur: Los casos de Argentina, Brasil, México y Venezuela. *Volumen 1. El Espacio Exterior: Una Oportunidad Infinita para Colombia*., 239.

Centro Criptológico Nacional. (2020). *Ciberamenazas y Tendencias—Edición 2020* (p. 44). https://n9.cl/6gqpx

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

Comando Conjunto Cibernético. (2020). *Marco normativo entorno digital*. CCC.

Comando Conjunto Cibernético. (2021). *Resumen de eventos cibernéticos, estadísticas y tendencias*. CCC.

Consejo Nacional de Política Económica y Social (CONPES). (2009). *Documento CONPES 3579 de 2009. Lineamientos para implementar el proyecto satelital de comunicaciones de Colombia*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social (CONPES). (2010). *Documento CONPES 3683 de 2010. Programa Satelital Colombiano*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social (CONPES). (2011). *Documento CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social (CONPES). (2020a). *CONPES 3983 de 2020. Política de Desarrollo Espacial*. Departamento Nacional de Planeación.

Consejo Nacional de Política Económica y Social (CONPES). (2020b). *CONPES 4001 de 2020. Declaración de importancia estratégica del Proyecto Nacional acceso universal a las tecnologías de la información y las comunicaciones en zonas rurales y apartadas*. Departamento Nacional de Planeación.

Crowdstrike. (2020). *Crowdstrike services cyber front lines report*. https://tinyurl.com/44267wds

Departamento Nacional de Planeación (DNP). (2019a). *Caracterización Mercado Satelital*. DNP.

Departamento Nacional de Planeación (DNP). (2019b). *Plan Nacional de Desarrollo 2018-2022*. DNP.

Falco, G. (2019). Cybersecurity principles for space systems. *Journal of Aerospace Information Systems, 16*(2), 61-70.

Falco, G. (2020). When satellites attack: Satellite-to-satellite cyber attack, defense and resilience. *ASCEND 2020*, 4014.

Federal Aviation Administration. (2021). *ADS-B Equipment*. https://www.faa.gov/nextgen/equipadsb/capabilities/ins_outs/

Fidler, D. P. (2018, abril). Cybersecurity and the new era of space activities. *Digital and Cyberspace Policy Program*.

Flórez, A. (2020). *Desarrollo de la industria espacial en el ámbito de la observación de la tierra en Colombia* [Tesis de Especialización en Administración Aeronáutica]. Universidad Militar Nueva Granada.

Fowler, B. W. (2016). *Cyber vulnerabilities in space systems*. Utica College.

Fuerza Aérea Colombiana (FAC). (2015). *Manual de Ciberseguridad y Ciberdefensa* [Manual]. Primera Edición. Ediciones FAC.

Fuerza Aérea Colombiana (FAC). (2020a). *Manual de Doctrina Básica Aérea, Espacial y Ciberespacial* (DBAEC) [Manual]. Quinta Edición. Departamento Estratégico de Doctrina Aérea y Espacial.

Fuerza Aérea Colombiana (FAC). (2020b). *Manual FAC-3.0-E Operaciones Aéreas, Espaciales y Ciberespaciales (MOAEC* - [Manual]. Departamento Estratégico de Doctrina Aérea y Espacial.

Fuerza Aérea Colombiana (FAC). (2020c). *Estrategia para el Desarrollo Aéreo y Espacial de la Fuerza Aérea Colombiana 2042*. https://www.fac.mil.co/sites/default/files/2021-04/edaes.pdf

Fuerzas Militares de Colombia (FF. MM.). (1996). *Manual de Seguridad y Defensa Nacional* [Manual]. Primera Edición. Imprenta y Publicaciones de las Fuerzas Militares.

Fuerzas Militares de Colombia (FF. MM.). (2018). *Manual Fundamental Conjunto (MFC 1.0) Doctrina Conjunta* [Manual]. Primera Edición. Imprenta y Publicaciones de las Fuerzas Militares.

Global Fishing Watch. (2021). *What is the Automatic Identification System (AIS)?* https://globalfishingwatch.org/faqs/what-is-ais/

Grisales, O. (2015). *Evolución de las nuevas amenazas a la Seguridad Nacional*. https://n9.cl/bimas

Hamilton, J. (2020). Cybersecurity in the Space Age. *ITNOW, 62*(2), 60-61.

Housen, D. (2016). Cybersecurity threats to satellite communications: Towards a typology of state actor responses. *Acta Astronáutica, 128*, 409-415.

Hutchins, R. (2016). *Cyber Defense of Space Assets*. Tufts School of Engineering. https://www.cs.tufts.edu/comp/116/archive/fall2016/rhutchins.pdf

Instituto Español de Estudios Estratégicos (IEEE). (2010). *Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio* [Manual]. http://www.ieee.es/Galerias/fichero/cuadernos/CE_149_Ciberseguridad.pdf

International Telecommunications Union. (2020). *Reglamento de Radiocomunicaciones*. ITU.

Javaid, A., Sun, W., Devabhaktuni, V., & Alam, M. (2012). Cyber security threat analysis and modelling of an unmanned aerial vehicle system. *2012 IEEE Conference on Technologies for Homeland Security (HST)*, 585-590.

Junta Interamericana de Defensa. (2020). *Guía de Ciberdefensa*. https://tinyurl.com/y36tkup6

Lane, D., Leon, E., Solio, D., Cunningham, D., Obukhov, D., & Tacliad, F. C. (2017). *High-assurance cyber space systems for small satellite mission integrity*. https://tinyurl.com/mr4xfc49

Latam Satelital. (2016). *Desarrollo satelital en Colombia, frustraciones y oportunidades*. https://tinyurl.com/5zfcsrph

Leopold, G. (2015). *Russian hacker group taps satellite links for attacks*. Defense Systems. https://tinyurl.com/54sbc2mk

Levi, R., & Dekel, T. (2012). *Space security national capabilities and programs, presentation at the space security conference 2011: Building on the past, stepping towards the future*. UNIDIR.

Lewis, J. A., Stone, L. F., Alonso, P., Fryer, M., Pires, J. C. L., Conroy, H., Scholl, L., Hernández, M. J., Maciel, O., & Molina, A. (2016). *Experiencias avanzadas en políticas y prácticas de ciberseguridad: Panorama general de Estonia, Israel, República de Corea y Estados Unidos*. BID.

Ley, W., Wittmann, K., & Hallmann, W. (2009). *Handbook of space technology* (Vol. 22). John Wiley & Sons.

Livingstone, D., & Lewis, P. (2016). *Space, the final frontier for cybersecurity?* Chatham House. The Royal Institute of International Affairs.

Llongueras, A. (2011). *La guerra inexistente, la ciberguerra*. Editorial Academia Española.

López, J. A. L. (2002). El poder aéreo, instrumento decisivo para la resolución de las crisis del siglo XXI. *Arbor, 171*(674), 231-257.

Manesh, M. R., & Kaabouch, N. (2019). Cyber-attacks on unmanned aerial system networks: Detection, countermeasure, and future research directions. *Computers & Security, 85*, 386-401.

Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2020). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, 1-25.

McKenna, A. T., Gaudion, A. C., & Evans, J. L. (2018). The role of satellites and smart devices: Data surprises and security, privacy, and regulatory challenges. *Penn St. L. Rev., 123*, 591.

Ministerio de las Tecnologías y la Comunicación [MinTIC]. (2020). *Análisis del Sector: Proyecto Centros Digitales* (N). MinTIC.

National Institute of Standards and Technology. (2018a). *NIST SP 800-37*.

National Institute of Standards and Technology. (2018b). *NIST SP 800-82*.

National Institute of Standards and Technology. (2020). *NIST SP 800-53*. Revisión 5.

OCDE. (2015). *The space economy at a glance 2014*. OECD Publishing.

OCDE. (2019). *The space economy in figures*. OECD Publishing.

Organización de las Naciones Unidas (ONU). (2002). *Tratados y Principios de las Naciones Unidas sobre el Espacio Ultraterrestre*. ONU.

OTAN. (2019). *Cybersecurity of NATO's space-based strategic assets*. Chatham House. The Royal Institute of International Affairs.

Santamarta, R. (2014). A wake-up call for satcom security. *Technical White Paper*.

Schmitt, M. (2017). *Tallinn Manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Smith, Z., Lostri, E., & Lewis, J. (2020). *The hidden costs of cybercrime*. McAfee.

Sundahl, M. (2013). Protocol to the Convention on International Interests in Mobile Equipment on Matters Specific to Space Assets. *The Cape Town Convention*, 223-249.

The Union of Concerned Scientists. (2021). *Satellite Database*. https://www.ucsusa.org/resources/satellite-database

Tovar, S. V., & Chávez, L. E. (2017). Ejercicio del ciberpoder en el ciberespacio. *Ciencia y Poder Aéreo, 12*(1), 236-244.

U. S. Department of Defense. (2018). *Summary Department of Defense Cyber Strategy*.

U. S. Satellite Industry Association. (2021). *State of the Satellite Industry Report 2021*.

Vargas, E. (2014). *Ciberseguridad y ciberdefensa: ¿qué implicaciones tienen para la seguridad nacional?* [Tesis]. Universidad Militar Nueva Granada. http://hdl.handle.net/10654/12259

Vera, T. (2016). *Cyber security awareness for smallsat ground networks*. https://digitalcommons.usu.edu/smallsat/2016/TS9GroundSystems/2/

Wang, G., Wei, S., Chen, G., Tian, X., Shen, D., Pham, K., Nguyen, T. M., & Blasch, E. (2016). Cyber security with radio frequency interferences mitigation study for satellite systems. *Sensors and Systems for Space Applications IX, 9838*, 98380K.

Capítulo 5

Poder multidominio: visión estratégica de la Fuerza Aérea Colombiana en el siglo XXI*

DOI: https://doi.org/10.25062/9786287602106.05

Carlos Enrique Álvarez Calderón
Yois Andrea Correcha Ramírez
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El capítulo tiene por objeto establecer cómo el espacio exterior y el ciberespacio son nuevos campos de batalla altamente reñidos y congestionados, donde se generan efectos a la velocidad de la luz. Esta disruptiva ampliación de los dominios de guerra tradicionales, potencializados por la tercera y cuarta revoluciones industriales, trae consigo retos y oportunidades paras las Fuerzas Militares (FF. MM.) de los Estados. Por lo tanto, este capítulo tiene por objeto proponer a la Fuerza Aérea Colombiana (FAC) la adopción de una visión de *poder multidominio*, que provea una mejor consciencia situacional y permita la rápida toma de decisiones por parte del comandante, así como el ágil despliegue de capacidades en los dominios del aire, el espacio y el ciberespacio en el siglo XXI.

Palabras clave: Ciberespacio, espacio exterior, poder aéreo, revolución de los asuntos militares.

* 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.

Carlos Enrique Álvarez Calderón

Magíster en Relaciones Internacionales de la Pontificia Universidad Javeriana y Magíster en Coaching Ontológico Empresarial de la Universidad San Sebastián (Chile). Politologo de la Pontificia Universidad Javeriana. Estudiante del Doctorado en Estudios Estrategicos, Seguridad y Defensa de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Becario del Centro de Estudios Hemisféricos de Defensa "William J. Henry". Docente Ocasional e Investigador Asociado Minciencias de la Maestría en Seguridad y Defensa Nacionales en la Escuela Superior de Guerra "General Rafael Reyes Prieto". Orcid: https://orcid.org/0000-0003-2401-2789 - Email: carlos.alvarez@esdeg.edu.co

Yois Andrea Correcha Ramírez

Teniente Coronel de la Fuerza Aérea Colombiana. Magister en Seguridad y Defensa Nacionales de la Escuela Superior de Guerra "General Rafael Reyes Prieto". Especialista en Defensa Aérea de la Escuela Militar de Aviacion "Marco Fidel Suarez". Ingeniera Electrónica de la Universidad Distrital "Francisco José de Caldas".ORCID: https://orcid.org/0009-0003-2862-7868 - Contacto: andrea.correcha@fac.mil.co

Citación APA: Álvarez Calderón, C. A. & Correcha Ramírez, Y. A. (2022). Poder multidominio: visión estratégica de la Fuerza Aérea Colombiana en el siglo XX. En F. Baquero Valdés (Ed.), *Poder aéreo, espacial y ciberespacial frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano* (pp. 209-249). https://doi.org/10.25062/9786287602106.05

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

En la actualidad, el complejo ambiente de seguridad y defensa de los Estados ha sido moldeado, entre otros factores, por cambios tecnológicos y una creciente interdependencia económica, social, política y militar que parece ya no estar limitada por fronteras geográficas. El espacio exterior y el ciberespacio son nuevos campos de batalla altamente reñidos y congestionados, donde se generan efectos a la velocidad de la luz. Por consiguiente, en la actualidad se combate en todos los dominios: aire, tierra, mar, espacio y ciberespacio. Esta disruptiva ampliación de los campos de batalla hace que el combate se traslade a través de los dominios, y sea conducido a una velocidad y con un alcance incrementales, desde el escenario táctico del combate cercano, atravesando teatros internacionales y alcanzando, incluso, el interior de un país.

Durante el último siglo, el poder aéreo ha sido testigo de dos desarrollos paralelos. El primero, predicho con precisión por H. G. Wells (1908), se relaciona con las capacidades de gran alcance del poder aéreo, en términos del alcance de las operaciones de combate, el logro de objetivos en tiempo real, las capacidades destructivas y una precisión notable. El segundo desarrollo es *mental*; es decir, una fe cada vez mayor en la capacidad autónoma del poder aéreo para el logro de objetivos militares y políticos que alguna vez requirieron, para su éxito, "botas sobre el terreno". Y resulta que el factor principal que impulsa este fenómeno parece ser la proliferación global de tecnología de información avanzada. La avalancha mundial de una tecnología comercial poderosa y fácilmente disponible exige un enfoque mucho más sofisticado para los asuntos militares. El catalizador principal de esta

revolución ha sido la miniaturización del transistor (el cual controla el flujo de electricidad en un circuito), lo cual permite que 20.000 millones de ellos se pongan en chips delgados de computador no más grandes que una uña. Como resultado, la potencia de procesamiento del computador se ha duplicado cada dos años, y se espera siga así en el futuro previsible (Álvarez & Ramírez, 2020). Esto ha creado un entorno de seguridad donde el ritmo de los avances cibernéticos, de energía dirigida, de nanotecnología, de robótica y de biotecnología está mucho más allá de la capacidad normal para predecir sus efectos.

Así, procurando su propia seguridad y defensa, y en desarrollo de las estrategias que a la satisfacción de sus intereses nacionales, actores estatales como Estados Unidos, China y Rusia usan una combinación de fuerzas convencionales, operaciones especiales y armas propias del ciberespacio, del espacio y electrónicas. Por otro lado, actores estatales y no estatales usan otros recursos adicionales para imponerse frente a sus adversarios, tales como la guerra de la información, las operaciones ambiguas o de negación de poder y la subversión (Álvarez & Jiménez, 2021). Terroristas, organizaciones criminales transnacionales y *hackers* cibernéticos, por mencionar algunos, han incrementado su capacidad, apoyados en la era de la información, que les permite ahora tener alcance global y masivo.

Ante este panorama, y proyectándose a futuro, las estrategias de seguridad y defensa de los Estados también se transforman respondiendo con la adopción de cambios estratégicos como el fortalecimiento de las relaciones, involucrando socios que proveen oportunidades para la cooperación (organizaciones multilaterales, organizaciones no gubernamentales [ONG], corporaciones, influenciadores estratégicos y asociaciones); también, mediante cambios que impactan el nivel operacional como la incorporación y el uso de las tecnologías emergentes, que incluyen computación avanzada, *Big Data*, analítica, inteligencia artificial (en inglés, AI, por las iniciales de *Artificial Intelligence*), autonomía, robótica, energía dirigida, hipersónicos y biotecnología, que buscan forjar la capacidad requerida para afrontar y vencer en las guerras del futuro.

Aunque Colombia ha experimentado cambios dramáticos en la tecnología, parece encontrarse tan solo en las etapas iniciales de comprender el impacto monumental de esta era en las futuras operaciones militares. Por consiguiente, y como parte de estos cambios y en procura de adaptarse al nuevo campo de batalla multidominio, surge para la FAC la necesidad de adoptar una visión de poder multidominio, que provea una mejor consciencia situacional y permita la

rápida toma de decisiones por parte del comandante, así como el ágil despliegue de capacidades en los dominios del aire, el espacio y el ciberespacio. A través de un Comando y Control Multidominio (MDC-2), los comandantes de la FAC podrían adaptarse con rapidez a las amenazas y las oportunidades, y crear efectos, a través de los dominios aéreos, espaciales y ciberespaciales, en el tiempo y el lugar necesarios y mediante el método escogido.

Del dominio aéreo al dominio ciberespacial

Antes de que se inventara el aeroplano, diversos escritores percibían que el espacio aéreo tenía características intrínsecas que podrían ser aprovechadas en la guerra. Por ejemplo, dos años antes de que los hermanos Wright realizaran sus primeros vuelos exitosos, H. G. Wells anticipaba, en 1901, una serie de invenciones a corto plazo que se aplicarían al campo de batalla en el siglo XX:

> La revolución que está en curso de la vieja a una nueva guerra, diferente en toda su naturaleza de la antigua, está marcada principalmente por el progreso constante en el alcance y la eficiencia del rifle y del cañón de campaña y más particularmente del factor aéreo […]. En la guerra que se desarrollará en el altamente organizado sistema de Estados europeos de este inicio de siglo, el globo militar utilizado junto con cañones, de pequeño calibre, pero de enorme longitud y alcance, desempeñará un papel de suma importancia. Estos cañones se llevarán en vastos carros mecánicos, posiblemente con ruedas de tal tamaño que les permitan atravesar casi todo tipo de terreno. Los aeronautas, provistos de mapas a gran escala del país hostil, señalarán a los artilleros en tierra el punto preciso sobre el cual dirigir su fuego, y sobre la colina y el valle, el proyectil volará, puede que diez millas, hasta su tocho, campamento, ataque nocturno masivo, o arma de avance. Grandes multitudes de globos serán los ojos de Argus de todo el organismo militar, ojos acechados con un nervio telefónico en cada tallo, y de noche barrerán el país con reflectores y volarán ante el viento con bengalas colgantes. (Wells, 1902, pp. 189-190)

No obstante, fue solo después de que los hermanos Wright realizaron su primer vuelo, en diciembre de 1903, cuando los militares empezaron a reconocer la utilidad que prometía el aeroplano como herramienta bélica. Y ya en 1911, durante la guerra entre Italia y el Imperio otomano, los aviones fueron utilizados en combate, por primera vez, sobre los cielos de Libia, donde se realizaron casi todas las misiones aéreas tradicionales: observación, defensa aérea, control del

espacio aéreo, transporte, ataques a blancos en tierra, y hasta bombardeos. En efecto, el 29 de septiembre de 1911, Italia declaró la guerra al Imperio otomano por el control de las provincias otomanas de Tripolitania y Cyrenaica: dos regiones que ahora componen la Libia moderna (Childs, 1990).

Ese mismo día, Italia desplegó una fuerza militar con una primera flotilla de aviones, formada por once pilotos y nueve máquinas primitivas; la mayoría, monoplanos. Luego, el 25 de octubre de 1911, la flotilla aérea italiana lanzó la primera misión de reconocimiento aéreo de la guerra, en medio de la cual patrullas aéreas italianas descubrieron el avance de las tropas turcas, lo que les permitió desplegar fuerzas terrestres que derrotaron a un enemigo desprevenido. Posteriormente, un piloto italiano llamado teniente Guilio Gavotti recibió la orden de lanzar granadas Cipelli desde su avión, para atacar los campamentos enemigos en los oasis de Ain Zara y Taguira. En consecuencia, la mañana del 1 de noviembre de 1911, y volando a 400 ft sobre el suelo, en un avión *Taube*, Gavotti dejó caer cuatro granadas Cipelli de 5 lb; y a pesar de que el ataque del teniente Gavotti causó pocas bajas, marcó un punto de inflexión en la guerra. Como era de esperarse, los bombardeos italianos también provocaron los primeros usos de armas de defensa aérea. Aunque en principio la resistencia otomana solo detentaba armas pequeñas que no eran rival para los aviones italianos, en la primavera de 1912, las fuerzas turcas en Azzizia montaron un cañón *Krupps* de 90 mm en un carro de gran altura, para disuadir los ataques enemigos; como respuesta, los pilotos italianos aumentaron su altura estándar de operaciones de 2.000 a 4.500 ft, en un ejemplo incipiente de guerra antiaérea.

En resumen, y a pesar de que el uso italiano del poder aéreo tuvo poco impacto en la guerra Ítalo-turca, señalaría el camino del uso del poder aéreo en las guerras por venir. La aviación italiana llevó a cabo una amplia variedad de misiones: bombardear posiciones turcas; localizar, fotografiar y filmar campamentos enemigos; interceptar trenes de camellos, y lanzar folletos de propaganda proitaliana, que ofrecían a los ciudadanos tripolitanos una moneda de oro y un saco de trigo si se rendían. Al final, los italianos lograron que las fuerzas otomanas capitularan, con el Tratado de Lausana, en octubre de 1912; en gran parte, porque el ejército italiano desplegó 100.000 soldados en el norte de África, que estaban mucho mejor entrenados y equipados que sus oponentes (Childs, 1990).

Como ocurrió durante la guerra en el norte de África, en 1911, durante la Primera Guerra Mundial (1914-1918), "la aviación había hecho acto de presencia en todas las funciones que configuran la guerra aérea en la actualidad: apoyo

directo desde el aire, reconocimiento, interdicción y defensa aérea, superioridad en el aire y bombardeo estratégico" (Álvarez et al., 2017, p. 167). No obstante, y a diferencia de la guerra entre Italia y el Imperio otomano, durante la Gran Guerra todas estas tácticas se utilizaron de manera más refinada, gracias al avance de la tecnología y a la mayor destreza de los pilotos. Por ejemplo, el reconocimiento aéreo condujo al apoyo aéreo cercano de las fuerzas combatiendo en tierra o en los mares, mientras que el creciente alcance de las aeronaves permitió a los estrategas aéreos pensar en función de interdicción, en bombardear las vías férreas que abastecían a las líneas enemigas. Y en la medida en que el alcance de las aeronaves fue mayor, en 1916, a los estrategas aéreos les fue posible pensar en función de atacar la capacidad bélica del enemigo (Álvarez, Benavides & Ramírez, 2019); y así comenzaron los limitados y primitivos bombardeos estratégicos, que, eventualmente, incentivaron la creación de las primeras fuerzas aéreas, como la Royal Air Force (RAF), en 1918.

Por lo tanto, ya para la Primera Guerra Mundial los atributos del poder aéreo incluían: 1) alcance: en 1918, hasta los aeroplanos más livianos podían volar cientos de kilómetros; 2) velocidad: más de 150 km por hora; 3) altitud (la capacidad para volar sobre montañas, ríos, y bosques; obstáculos que, por el contrario, impedían el avance de las fuerzas de superficie), y 3) capacidad letal (la concentración de fuego podía dirigirse a puntos específicos en el frente de batalla o detrás de las líneas enemigas). Pero las limitaciones del poder aéreo también se hicieron evidentes en las primeras dos décadas del siglo XX.

A diferencia de las fuerzas terrestres, los aviones militares no podían permanecer indefinidamente en su medio, y tenían que aterrizar para reaprovisionarse de combustible y de municiones. Estas limitaciones, a su vez, hacían que el uso de los aeroplanos fuese efímero, y los ataques aéreos solo duraban unos cuantos minutos; por ende, carecían de persistencia. Asimismo, los aviones de la época aún estaban limitados por el mal tiempo y la oscuridad de la noche, y en una guerra que aún se basaba en la adquisición de territorios, la aviación por sí sola no podía ocupar o mantener territorios conquistados. Por ello, a pesar de sus promesas, el poder aéreo no jugó tampoco un rol decisivo en el desenlace de la Primera Guerra Mundial.

Sin embargo, durante la Segunda Guerra Mundial (1939-1945), el rol del poder aéreo sería decisivo; sobre todo, en lo concerniente al bombardeo estratégico contra centros de población civiles y la infraestructura critica del adversario (Álvarez et al., 2017). En efecto, todas las principales partes en conflicto,

como la Lutwaffe (Fuerza Aérea nazi), la RAF (británica), la United States Army Air Forces (Aviación del Ejército estadounidense), la Regia Aeronautica Italiana (Fuerza Aérea del Reino de Italia), la Voyenno-Vozdushnyye Sily (Fuerza Aérea soviética) y la Dai-Nippon Teikoku Rikugun Kōkū-butai y la Dai-Nippon Teikoku Kaigun Kōkū-butai (Servicio Aéreo del Ejército y de la Armada Imperial japonesa), participaron activamente en misiones de bombardeo a lo largo del conflicto, ya que al destruir industrias esenciales, como las centrales eléctricas o las fábricas de rodamientos, el bombardeo aéreo podía paralizar la actividad industrial del enemigo. Asimismo, el uso de bombarderos en combinación con cazas de largo alcance, como el P-51 "Mustang", ejercieron un impacto significativo sobre la moral del enemigo y obligaban a destinar para la defensa aérea recursos materiales y humanos que, de otra manera, habrían podido ser utilizados en el frente de combate.

Por consiguiente, el uso sistemático del dominio aéreo en la Segunda Guerra Mundial fue decisivo para los principales esfuerzos de la guerra, en la cual la velocidad, la movilidad y la sorpresa jugaron un papel dominante de la doctrina militar de aquel momento (por ejemplo, la *Blitzkrieg* alemana o la *Kido Butai* japonesa), y determinarían el patrón para imitar en los conflictos del futuro. Es más, una vez terminada la Segunda Guerra Mundial, en 1945, se estableció formalmente que las operaciones militares en distintos ambientes físicos requerían conocimientos especializados y experiencia técnica que justificaban tres ramas funcionales separadas.

En consecuencia, los Estados que se preciaran de contar con FF. MM. modernas debían crear una Fuerza Aérea como componente autónomo de sus Fuerzas Armadas (FF. AA.). Y fue la necesidad de contar con capacidades cada vez más sofisticadas para el "control de las alturas" lo que produjo la carrera aeroespacial entre Estados Unidos y la Unión Soviética durante la Guerra Fría (1947-1991), y lo que amplificó el poder aéreo al dominio espacial. Como lo señalan Álvarez, Murillo y Hernández (2019), desde el lanzamiento del *Sputnik*, por parte de la Unión Soviética, en 1957, "muchos Estados comenzaron a incluir las preocupaciones de seguridad basadas en el espacio en sus políticas exteriores, lo que les obligó a considerar qué significaban las nuevas operaciones en el espacio para la seguridad nacional" (p. 75).

A partir de la puesta en órbita terrestre del primer satélite espía del programa *Corona*, desarrollado por la Agencia Central de Inteligencia (CIA) y la Fuerza Aérea estadounidense a finales de la década de 1950, o del primer uso de un

sistema de satélites para la navegación de la armada estadounidense, a comienzos de la década de 1960, así como del desarrollo de satélites de alerta temprana de misiles balísticos intercontinentales y satélites de comunicaciones, a comienzos de la década de 1970, el uso militar del dominio espacial empezó a considerarse un invaluable multiplicador de las fuerzas de aire, tierra y mar. Sumado a ello el avance en la capacidad de los computadores y el mayor desarrollo de la cibernética, para la última década del siglo XX, la integración de algunas capacidades áreas, espaciales y ciberespaciales permitió el ejercicio de una violencia más precisa por parte de las fuerzas aéreas más modernas, como quedó en evidencia con: la Operación Tormenta del Desierto (1990-1991), en Irak; la Operación Fuerza Deliberada (1995), en Bosnia, y la Operación Fuerza Aliada (1999), en Kosovo.

En efecto, la Revolución de los asuntos militares[1] (RAM), de principios de la década de 1990, consistió en la sinergia entre tres elementos: 1) capacidades de inteligencia, vigilancia y reconocimiento de vanguardia; 2) recursos avanzados de comando, control, comunicación e informática, y 3) municiones de largo alcance guiadas con precisión. Si bien en 1943, tanto Estados Unidos como Alemania comenzaron a emplear armas inteligentes —dirigidas contra blancos fijos mediante señales de radio, enviadas, a su vez, desde la plataforma de lanzamiento—, en 1958 Estados Unidos empezó, además, a utilizar misiles de precisión guiados contra objetivos móviles; incluso, hacia finales del decenio de 1960 entraron en servicio los primeros misiles del tipo "dispara y olvida", que no requerían ser guiados por una persona.

Y pese a que los satélites espaciales se utilizaron por primera vez en labores de reconocimiento en 1961, y para comunicaciones, en 1965, y a que los primeros computadores tácticos entraron en uso en 1966, y el primer correo electrónico se envió en 1972, lo cierto es que cada uno de esos elementos se había empleado operativamente de manera aislada, hasta cuando en

1 El concepto de RAM fue acuñado a fines de la década de 1970, por el mariscal Nikolai V. Ogarkov, jefe del estado mayor soviético. El concepto de RAM se afianzó en Estados Unidos cuando el Office of Net Assessment del Pentágono ordenó un importante estudio de la teoría rusa, a la luz de la experiencia de la guerra del Golfo, de 1991. El informe, publicado en 1992, concluía que, en efecto, se estaba llevando a cabo un RAM, en el cual ejércitos masivos serían reemplazados por fuerzas más pequeñas y profesionales con mayor potencia de fuego, y los cuales lucharían a distancia, en vez de acercarse y destruir al enemigo (Krepinevich, 1992). Por consiguiente, el Office of Net Assessment del Departamento de Defensa de los Estados Unidos define un RAM como un cambio importante en la naturaleza de la guerra, provocado por la aplicación innovadora de tecnologías que, combinadas con cambios dramáticos en la doctrina militar y los conceptos operativos, altera en lo fundamental el carácter y la conducción de las operaciones militares.

la Operación Tormenta del Desierto los militares estadounidenses integraron esas innovaciones en un gran *sistema de sistemas*[2]. Desde la codificación de la fuerza conjunta, con la Ley Goldwater-Nichols, en 1986, Estados Unidos usaría la estructura de fuerza de tarea conjunta combinada con sus socios de coalición para hacer la guerra; no obstante, dicha estructura y su doctrina subyacente fueron usadas por primera vez durante la Operación Tormenta del Desierto, en 1991.

Y ya que los avances tecnomilitares no se han detenido, la fusión de los dominios aéreo, espacial y ciberespacial ha cobrado mayor importancia en el siglo XXI, como lo atestiguan la Operación Libertad Iraquí (2003-2005); la Operación Resolución Inherente (2014-2019), en Siria, Irak y Libia, y la Operación Libertad Duradera (2001-2021), en Afganistán. Los resultados operacionales de las misiones aéreas llevadas a cabo en estos conflictos han consolidado la percepción de que el ataque aéreo es un medio eficaz para afectar la voluntad del adversario, reducir el propio número de bajas, ocasionar menos daños colaterales y permitir mayores ahorros presupuestarios.

Como parte del actual esfuerzo de modernización, las fuerzas aéreas de diversos Estados ahora ponen mayor énfasis en capacidades ofensivas autónomas y en el uso de activos espaciales y contraespaciales, así como en un mayor aprovechamiento del ciberespacio. Es un objetivo que, evidentemente, incluye el desarrollo de equipos más modernos; en particular, cazas y bombarderos furtivos, vehículos aéreos remotamente tripulados (VART), sistemas de alertas tempranas avanzadas, y un mejor comando y control, comunicaciones, computadores e inteligencia, vigilancia y capacidades de reconocimiento (en inglés, C4ISR, por las iniciales de *Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*). Estos programas de modernización de la Fuerza y los habilitadores que se relacionen con ellos están destinados

2 Washington esperaba que la guerra del Golfo se desarrollaría de manera tradicional. En diciembre de 1990, pronosticaron una violenta confrontación militar terrestre; posiblemente, con la mayor batalla de tanques en la historia de la guerra, por lo cual se anticipó que las fuerzas terrestres serían decisivas, mientras que el poder aéreo sería un elemento de apoyo. La Fuerza Aérea estadounidense (USAF) inició el ataque a las 3:00 a. m. del 17 de enero de 1991, y para el amanecer de ese día, la red de comando y control de Irak había sido destruida. Luego, una campaña aérea de 38 días dejó a las fuerzas iraquíes casi destruidas, incapaces de realizar operaciones coherentes, por lo cual fueron rematadas en una acción terrestre de 100 horas y cuatro días (Dorr, 2011). Los ataques de precisión desde el aire y la superioridad de la información establecieron un nuevo estándar de efectividad, y posibilitaron al poder aéreo de la coalición la destrucción de 150 objetivos individuales tan solo el primer día de la guerra (Weitz, 2004). A partir de entonces, el concepto de RAM incluía todas las armas de combate, pero se identificaba cada vez más con el poder aéreo; y los posteriores conflictos regionales en Bosnia (1995) y Serbia (1999) dieron mayor credibilidad a esa conclusión.

a mejorar las capacidades de combate de una fuerza aérea, y a convertirla en un instrumento más poderoso de disuasión y diplomacia coercitiva que permita a un Estado lograr sus intereses nacionales, tanto objetivos como subjetivos (Álvarez et al., 2018).

La tecnología de información avanzada también está cambiando las perspectivas de interdependencia multidominio. La capacidad para proyectar poder convencional en el ámbito doméstico o en el foráneo se está erosionando rápidamente, a medida que actores estatales y no estatales adquieren capacidades avanzadas para compensar las propias capacidades. Esto ocurre en prácticamente todos los dominios operativos: aire, tierra, mar, espacio y ciberespacio. Además, el requisito de pensar en todos los dominios se produce cada vez más en los niveles inferiores de la estrategia, como en el de la estrategia militar operativa y el de la táctica. Estos cambios en el entorno operativo, combinados con "nuevas" realidades fiscales, están transformando rápidamente la forma como debe pensarse en las amenazas, el espacio de batalla y los fundamentos conceptuales del poder aéreo. Pero si algo es indiscutible es que en el ambiente operacional (OE), cada vez más complejo y controvertido, del futuro, el planteamiento óptimo de conducción de la guerra para las FF. AA. colombianas debe centrarse en las operaciones en múltiples dominios.

El concepto de dominio

Antes del uso generalizado del concepto *dominio*, las operaciones militares se describían típicamente en solo tres dimensiones físicas, de tierra, mar y aire; esta noción de tres dimensiones físicas se convirtió en el principio organizativo básico de las FF. AA. en tres ramas separadas: Ejército, Armada y Fuerza Aérea. Pero según Heftye (2017), durante las dos últimas décadas, el uso de la palabra *dominio* ha logrado una amplia aceptación en el léxico militar, ya que crea un "marco de referencia que define la preparación y conducción de la guerra. Cada institución y servicio militar elabora doctrinas y plataformas que están diseñadas para operar o maniobrar en su dominio dominante" (Hoffman & Davies, 2013).

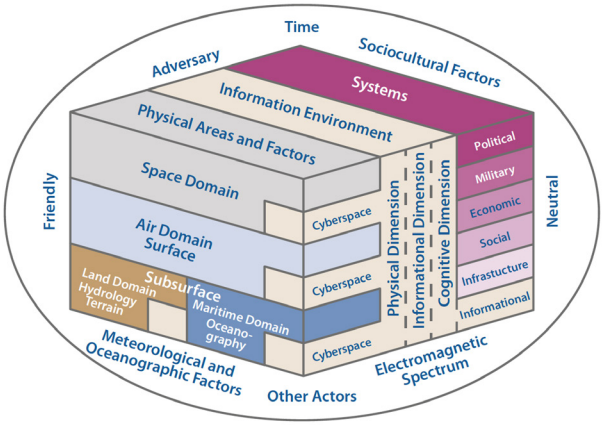
En principio, la Real Academia de la Lengua Española (RAE) define "dominio" como: 1) el poder que alguien tiene de usar y disponer de lo suyo, y 2) el ámbito real o imaginario de una actividad. No obstante, y para el contexto de las operaciones militares, un *dominio* se refiere a los espacios físicos y no físicos en los cuales se llevan a cabo operaciones militares; es decir, el "ámbito de

operación" de las FF. MM. de un Estado[3]. En este orden de ideas, el Centro de Doctrina Conjunta de las Fuerzas Militares de Colombia (CEDCO) define dominio como una "construcción doctrinal empleada en la conducción de operaciones y campañas para describir, visualizar y caracterizar el ambiente" (CEDCO, 2018, p. 35). Por su parte, el Departamento de Defensa de Estados Unidos lo define como "cualquier espacio operacional potencial a través del cual el sistema objetivo pueda ser influenciado —no solo los dominios de tierra, mar, aire y espacio, sino además del dominio virtual (información y ciber) y el humano (cognitivo, moral, juicios de valor y social)" (US Department of Defense, 2005, p. 16). Cabe señalar que la doctrina conjunta de Estados Unidos no determina los límites precisos para cada dominio, lo cual resulta complejo; sobre todo, a la hora de precisar los ámbitos no físicos (ciberespacio y cognitivo), ya que carecen de límites tangibles; mientras los dominios físicos involucran material real, tanto el ciberespacio como el espectro electromagnético son dominios *virtuales* que involucran las acciones de sensar y percibir.

Sin embargo, el Manual de Doctrina Conjunta MFC 1-0 de las Fuerzas Militares de Colombia no solo reconoce cinco dominios en los cuales se desarrollan las acciones militares, sino que también los delimita (CEDCO, 2018): 1) *dominio terrestre*: área de la superficie de la Tierra que termina en el nivel del mar y se superpone con el dominio marítimo en el segmento de los litorales; 2) *dominio marítimo*: los océanos, los mares, las bahías, los estuarios, las islas, las zonas costeras y el espacio aéreo por encima de estos, incluidos los litorales; 3) *dominio aéreo*: la atmósfera, que comienza en la superficie de la Tierra y se extiende hasta la altura donde sus efectos sobre las operaciones se hacen insignificantes; 4) *dominio espacial*: ambiente donde la radiación electromagnética, las partículas cargadas y los campos eléctricos y magnéticos son las influencias físicas dominantes, y abarcan la ionósfera y la magnetósfera de la Tierra, el espacio interplanetario y la atmósfera solar; 5) *ciberespacio*: dominio global dentro del ambiente de la información, consistente en redes interdependientes de infraestructura de tecnologías de la información y datos contenidos que incluyen: internet, telecomunicaciones, redes, sistemas informáticos y procesadores y controladores integrados.

3 Según el Diccionario de la Lengua Española de la RAE, un *ámbito* se define como "contorno o perímetro de un espacio o lugar" o como "espacio dentro de ciertos límites".

Figura 1. *Vista holística del ambiente operacional (Manual JP-5.0).*



Fuente: US Joint Force Development (2017).

Características de un dominio

Allen y Gilbert (2009) definen un dominio como una "esfera de interés e influencia en la que se llevan a cabo actividades, funciones y operaciones para cumplir misiones y ejercer control sobre un oponente con el fin de lograr los efectos deseados"[4]. Al desglosar esta definición, Allen y Gilbert (2009) respaldan que cada uno de los cinco dominios existentes (tierra, mar, aire, espacio y ciberespacio) califican como un dominio, ya que son: 1) una esfera de interés; 2) una esfera de influencia en la que pueden realizarse actividades, funciones y operaciones para cumplir misiones; 3) una esfera que puede incluir la presencia de un oponente, y 4) una esfera en la que se puede ejercer control sobre ese oponente. En efecto, cada uno de los cinco dominios tiene su propia esfera de interés e influencia, y en cada uno de dichos dominios, un oponente puede estar presente y puede interferir con las operaciones amigas. Además, los Estados vienen fortaleciendo sus capacidades militares en cada uno de esos dominios, las cuales pueden utilizarse para controlar y dominar a posibles adversarios.

Asimismo, Allen y Gilbert (2009) sugieren que existen seis características clave a la hora de valorar un dominio: 1) se requieren capacidades únicas para operar en un dominio; 2) un dominio no es completamente abarcado por ningún

4 Con base en esta definición, Álvarez et al. (2017) reconocerían que, en el marco de guerras de quinta generación, los dominios se agrupan típicamente en tres categorías más grandes: *físicos* (aéreo, espacial, terrestre, marítimo), *digital* (ciberespacial, espectro electromagnético, información, nuevas tecnologías) y *cognitivo* (desinformación, psicológica, comunicaciones estratégicas).

otro dominio; 3) es posible una presencia compartida de capacidades amistosas y adversarias en el dominio; 4) se puede ejercer control sobre el dominio; 5) un dominio brinda la oportunidad de sinergia con otros dominios, y 6) un dominio brinda la oportunidad de realizar acciones asimétricas en todos los dominios. Con base en lo anterior, Allen y Gilbert (2009) postulan que si un dominio tiene estas seis características, califica como dominio, pero si no tiene las seis características, no debería calificar como dominio. Los siguientes ejemplos demuestran cómo los cinco dominios de tierra, mar, aire, espacio y ciberespacio califican como un dominio, de acuerdo con estas seis características:

1. **Se requieren capacidades únicas para operar en un dominio especifico:** Por ejemplo, las aeronaves deben operar en el dominio aéreo; las naves espaciales, en el dominio del espacio exterior; los barcos, en el dominio marítimo, y los sistemas terrestres, en el dominio terrestre. También se requieren capacidades cibernéticas para operar en el ámbito del ciberespacio, ya que este dominio requiere equipos y habilidades de personal especializados para funcionar con eficacia, cumplir misiones y dominar cualquier presencia enemiga. Es decir, las capacidades cibernéticas que operan en el ciberespacio son únicas y diferenciables de las capacidades diseñadas para operar en otros dominios; por ejemplo, un sistema informático y el *software* o el código asociado para hackear redes informáticas enemigas es un activo diferente de las plataformas aéreas, terrestres, marítimas y espaciales. Por lo tanto, las habilidades de un *cibersoldado* son tan especiales para operar, defender e intentar dominar el dominio de manera efectiva como las de un piloto, un marino, un soldado o un astronauta en sus dominios respectivos.
2. **Un dominio no es completamente abarcado por ningún otro dominio único:** Por ejemplo, el dominio aéreo no es abarcado por el dominio terrestre, ni viceversa. Las capacidades, las misiones y las técnicas de cada dominio siguen siendo únicas. Un tanque no está diseñado para operar en el dominio aéreo, mientras que un avión no está diseñado para operar bajo el agua. De igual manera, el ciberespacio no es completamente abarcado por ninguna combinación de los dominios terrestres, marítimos, aéreos o espaciales, por cuanto tiene capacidades y funciones que son significativas solo para ese dominio.
3. **Es posible una presencia compartida de capacidades amistosas y adversarias:** Cualquier dominio puede ser "ocupado" por fuerzas adversarias. Esto no quiere decir que todos los oponentes se hallen presentes en todos los dominios, sino que debe ser posible una presencia contraria para que la esfera

de interés e influencia se considere un dominio. Una presencia potencial compartida es una característica esencial de un dominio, ya que el dominio o el control sobre el dominio requieren la posibilidad de una presencia o una capacidad adversarias.

4. **Se puede ejercer control:** La presencia de un oponente potencial en la esfera de interés genera la necesidad de influir o dominar a dichos oponentes en un dominio. Dado que un dominio es una esfera de influencia y de interés, entonces debe ser posible que la influencia de una parte en un dominio domine la influencia de la contraparte. En el caso del ciberespacio, el control puede referirse al control de los sistemas de información, el control del acceso a la información o, incluso, el dominio de una creencia sobre otra en el escenario cognitivo; por ejemplo, los radares aire-aire en aviones de combate pueden intentar bloquear o falsificar los radares de fuerzas opuestas en el dominio aéreo, e intentar así controlar el acceso a la información. La reciente avalancha de ataques cibernéticos patrocinados por algunos Estados a algunos sistemas de información sensibles de Colombia es un ejemplo del tipo de control temporal que los adversarios pueden llevar a cabo en el dominio del ciberespacio; pero, asimismo, las actividades de desinformación e influencia a través del ciberespacio que afectan las creencias de una sociedad es una batalla de ideas que compiten por el dominio sobre otras ideas.
5. **Brinda oportunidades de sinergia:** Las capacidades en un dominio deben brindar oportunidades sinérgicas con capacidades en otros dominios. Por ejemplo, los dominios espacial y ciberespacial proporcionan apoyo sinérgico a todos los otros dominios, y viceversa; la capacidad para recopilar información del enemigo a través de la observación de activos espaciales, o directo de una fuente de información, a través del ciberespacio, puede ayudar a las operaciones aéreas, terrestres y marítimas.
6. **Proporciona oportunidades asimétricas:** Similares a las oportunidades sinérgicas son las oportunidades para que las capacidades en un dominio obtengan una ventaja asimétrica sobre las fuerzas opuestas en otros dominios. Por ejemplo, la oportunidad de utilizar activos aéreos como una amenaza asimétrica contra activos terrestres y marítimos del adversario, mientras que pueden utilizarse fuerzas terrestres o marítimas para amenazar asimétricamente los activos aéreos del enemigo. El principio de asimetría debe ser una posibilidad de capacidades en una esfera de interés para que sea definida como dominio.

Donnelly y Farley (2019) definen un dominio como aquel "espacio de macro maniobra crítico cuyo acceso o control es vital para la libertad de acción y superioridad requerida por la misión". Con base en esta definición, un dominio empieza con una maniobra; es decir, con un "conjunto de tareas y sistemas relacionados entre sí que mueven y emplean las fuerzas para ganar una posición de ventaja relativa sobre el enemigo y otras amenazas" (CEDCO, 2018, p. 69). De acuerdo con Donnelly y Farley (2019), la maniobra en un dominio es a menudo una característica única y definitoria que separa los dominios entre sí, aunque la maniobra *per se* no es suficiente para un dominio; por consiguiente, el término *macro* ayuda a simplificar la definición al imponer cierto nivel de restricción, ya que, sin *macro* se podría argumentar que cualquier rasgo distintivo constituiría un nuevo dominio.

El siguiente segmento de la definición de Donnelly y Farley (2019) es "cuyo acceso o control es vital". Al igual que la proposición de Allen y Gilbert (2009), esto implica la necesidad de acceso o control de un medio para que sea catalogado como un dominio; por ejemplo, antes del lanzamiento del *Sputnik*, en 1957, el dominio espacial existía físicamente, pero no era accesible desde el punto de vista operativo. Por ello, si la capacidad de maniobrar, acceder o controlar un medio es vital para la misión, entonces cumple con la definición de dominio. El segmento final de la definición de Donnelly y Farley (2019) es "libertad de acción y superioridad requeridas por la misión". Se refiere, entonces, a la misión y a la capacidad para actuar libremente y obtener superioridad en un dominio; por ende, la superioridad puede venir en forma de acceso o negación de un dominio, como ocurre en la superioridad aérea, espacial o ciberespacial.

En este orden de ideas, la FAC maniobra en tres dominios para lograr la superioridad y la libertad de acción: dos físicos (aéreo y espacial) y uno virtual (ciberespacio). De acuerdo con el Manual de Doctrina Básica Aérea, Espacial y Ciberespacial (DBAEC) 5a Edición de la FAC,

> Dominar el aire, el espacio y el ciberespacio se define como la capacidad de la FAC para actuar de forma separada, conectada, combinada o reconfigurada en el aire, el espacio y el ciberespacio, en contra de todo tipo de amenaza para conseguir los efectos deseados explotando los siguientes elementos: flexibilidad, velocidad, coordinación balance y fuerza. Alrededor de esta función se desarrollan todas las demás, de hecho, se considera como un requisito previo para que se obtenga la libertad de acción del poder militar como un todo. (Fuerza Aérea Colombiana [FAC], 2020a, p. 10-2)

Por lo expuesto, es importante tener claridad en los términos que vayan a emplearse, pues influyen en la constitución de las categorías mentales y en las percepciones, las preferencias y las prioridades que determinan la acción humana. En la actualidad, la FAC busca incorporar en su doctrina el concepto *poder multidominio*, para lo cual no solo es importante definir que se entiende por "poder dominio", sino diferenciarlo de otro concepto militar que ha influenciado la doctrina militar conjunta: las *operaciones multidominio*.

Operaciones multidominio: una evolución de las operaciones conjuntas

En 2018, el Comando de Doctrina y Entrenamiento del Ejército de Estados Unidos (US Army TRADOC) definió las operaciones multidominio como[5]

> Aquellas que se llevan a cabo en múltiples dominios y espacios impugnados para superar las fortalezas de un adversario (o enemigo), presentándolos con varios dilemas operativos y/o tácticos a través de la aplicación combinada de la postura de la fuerza calibrada; empleo de formaciones multidominio; y convergencia de capacidades en dominios, entornos y funciones en el tiempo y los espacios para lograr objetivos operativos y tácticos. (US Army TRADOC, 2018, p. 7)

Pero el concepto de operaciones entre dominios no es nuevo, ya que ha sido una parte inherente del pensamiento militar desde la Antigüedad. La fallida campaña ateniense para conquistar Sicilia durante la guerra del Peloponeso (431 a. C.-404 a. C.) es solo un ejemplo de ello. En efecto, Atenas lanzó en 415 a. C. una expedición para someter a Siracusa, la ciudad-Estado más fuerte de Sicilia. La fuerza ateniense, liderada por Nicias, consistía en aproximadamente 6.400 hombres y 134 barcos. Y si bien los atenienses disfrutaron de los primeros éxitos operaciones de dicha campaña militar, en 414 a. C., durante el asedio de Siracusa, el general espartano Gilipo intervino y cambió el rumbo de la batalla a favor de las fuerzas de Siracusa. Gilipo se concentró inicialmente en el dominio humano inspirando a las fuerzas

5 La USAF ofrece otra definición para las operaciones multidominio; como lo señalan Grest y Heren (2019), dicha definición va orientada al propio ámbito de actuación de la USAF: "ejecución coordinada de autoridad y dirección para ganar, fusionar y explotar información desde cualquier fuente, para planeamiento integrado y ejecución sincronizada de operaciones multidominio en el tiempo, espacio y propósito para lograr los objetivos del comandante" (USAF, 2015).

siracusanas y estimulando el apoyo de sus aliados, para luego atacar simultáneamente a las tropas atenienses en tierra y en el mar. Para 413 a. C., los atenienses habían sido derrotados.

Esta derrota marcó el principio del fin para el Imperio ateniense, porque exacerbó el pánico en Atenas, lo cual provocó un cambio importante en las alianzas atenienses y allanó el camino para la victoria final de Esparta sobre Atenas, en 404 a. C[6]. Sin embargo, según Reilly (2019), la lección de este ejemplo histórico va mucho más allá del colapso de Atenas, por cuanto destaca la importancia de comprender los múltiples dominios y la necesidad de cambiar la superioridad local entre dominios. Es importante anotar que Gilipo y las fuerzas de Siracusa no tuvieron éxito en todos sus enfrentamientos; de hecho, los atenienses derrotaron o repelieron a esas fuerzas en varios puntos clave de la campaña. Sin embargo, Gilipo comprendía que la superioridad en cualquier dominio puede no ser generalizada o permanente, sino más frecuentemente local y temporal, por lo cual la comprensión de Gilipo de la importancia de vincular múltiples dominios y operar a través de estos, fue el elemento intrínseco en la victoria de Siracusa. La lección de Gilipo es que establecer la superioridad en una combinación de dominios ofrece la libertad de acción necesaria para alcanzar el éxito de la misión.

Otro ejemplo que demuestra la importancia de las operaciones multidominio fue una batalla de la Segunda Guerra Mundial. El 7 de agosto de 1942, las fuerzas estadounidenses desembarcaron en la isla de Guadalcanal, en el archipiélago de las islas Salomón, en el Océano Pacífico. Después de establecer el control del aeródromo en la isla, que nombraron aeródromo "Henderson", la misión de los estadounidenses cambió de impedir un desembarco japonés en la isla a sostener y reforzar las fuerzas de su país que ya estaban en Guadalcanal (Bruce, 2006). Como las dos bases principales en el área (Rabaul, para Japón, y Espíritu Santo, para Estados Unidos) se encontraban a una distancia de 900 km de la isla, bien podría parecer que esta fue una batalla en el dominio marítimo, aunque, realmente, para alcanzar la victoria, ambas partes usaron una variedad de esfuerzos "multidominio" intentando forzar y mantener abiertas las rutas de acceso a Guadalcanal.

6 El control de Siracusa fue un también un punto de inflexión en las guerras Púnicas (264 a.C-146 a. C.), entre el Imperio romano y el cartaginés. Ambas partes en contienda también emplearon operaciones multidominio en la segunda guerra Púnica (219 a. C.-201 a. C.), caracterizadas por el uso de fuerzas terrestres y navales. Al final, Roma logró imponerse a Cartago, y consolidar así su hegemonía sobre la cuenca del Mediterráneo (Álvarez & Botero, 2021).

Para los estadounidenses, estas operaciones se centraron en impedir que los convoyes japoneses transportaran tropas y abastecimientos de Rabaul a Guadalcanal. Las operaciones aéreas del aeródromo Henderson participaron en el dominio marítimo, lo cual obligó a los transportes nipones a moverse de noche dentro de la cobertura aérea estadounidense, que hizo más difícil la navegación y la manipulación de la carga. Asimismo, las fuerzas aéreas apoyaron los esfuerzos en el dominio terrestre para aumentar y proteger el perímetro del aeródromo Henderson de cualquier ataque japonés. Al mismo tiempo, las fuerzas navales estadounidenses participaron en el dominio terrestre, con el apoyo de fuego naval, el hostigamiento de fuerzas terrestres niponas e interdicción de abastecimientos cuando se movían hacia y alrededor de la isla de Guadalcanal. Las fuerzas navales también "entraron" en el dominio aéreo con el uso de aviones basados en portaaviones, para atacar los portaaviones japoneses y neutralizar las redadas aéreas de estos contra el aeródromo Henderson, así como la interrupción de esfuerzos japoneses de bombardear la isla desde el mar. Por su parte, las fuerzas terrestres influyeron en el combate marítimo a través de observadores costeros, que proporcionaron inteligencia sobre los movimientos navales y aéreos de Japón, así como la defensa del aeródromo Henderson contra ataques terrestres y bombardeos de artillería nipona.

Los japoneses también se involucraron en operaciones multidominio, ya que sus fuerzas aéreas en Rabaul amenazaron los buques estadounidenses en el mar, y así limitaron las áreas donde la Armada de Estados Unidos podía operar con seguridad. Los japoneses también atacaron posiciones terrestres enemigas en la isla. Simultáneamente, las fuerzas navales de los nipones apoyaron las operaciones terrestres escoltando buques de transporte a la isla y hundiendo varios buques de guerra de Estados Unidos que habían intentado establecer un bloqueo de la isla, y participaron con bombardeos al aeródromo Henderson desde el mar. Las fuerzas terrestres japonesas trataron varias veces de asaltar dicho aeródromo, lo que habría podido darles el control del espacio aéreo sobre la isla para permitir el movimiento marítimo de abastecimientos. Pero al final, la capacidad de las FF. MM. de Estados Unidos y sus aliados para coordinar sus actividades multidominio les permitieron disfrutar los beneficios sinérgicos de operar a través de los dominios. Los nipones lograron un menor nivel de éxito en su capacidad para unir los elementos terrestres, aéreos y navales en una operación militar cohesiva, en comparación con los de Estados Unidos, y con el tiempo perdieron Guadalcanal y otras islas, como consecuencia de ello.

El Proceso de Comando y Control

Y así como ha ocurrido en otros tiempos, las operaciones multidominio pueden constatarse en los actuales campos de batalla. Por ejemplo, las operaciones aéreas han realizado avances significativos a fin de fusionar el espacio, el aire y algunos efectos cibernéticos para apoyar las operaciones conjuntas. Hay un progreso similar en las operaciones espaciales, terrestres y marítimas, aunque, de acuerdo con Carlisle (2019), todavía se presentan algunas dificultades a la hora de encontrar la mejor manera de incorporar el Comando y Control (C2)[7] cibernético en todos los centros de operaciones, al igual que en la comunidad de inteligencia. Aunque el propósito del C2 no ha cambiado desde cuando las primeras FF. MM. empezaron a enfrentarse entre sí, la forma como se entiende el C2 y los medios por los cuales se cumplen sus funciones sí han cambiado significativamente a lo largo de la historia. Estos cambios han ido de la mano de la tecnología, la naturaleza de las operaciones militares, las capacidades de las fuerzas y los entornos en los que operan los ejércitos.

En este sentido, David Alberts y Richard Hayes desarrollaron en 1942 el primer modelo conceptual del C2; para los autores, el C2 no es un fin en sí mismo, pero es un medio para crear valor (por ejemplo, el cumplimiento de una misión). Específicamente, el C2 consiste en "enfocar los esfuerzos de una serie de entidades (individuos y organizaciones) y recursos, incluida la información, hacia el logro de alguna tarea, objetivo o meta" (Alberts & Hayes, 2006, p. 32). Para Alberts y Hayes (2006), un C2 tradicional presenta las siguientes características: 1) hay alguien reconocido por estar "a cargo"; 2) existe una única cadena de comando; 3) existe doctrina que define los patrones de interacción, y 4) la distribución de información sigue la cadena de comando.

Empero, Alberts y Hayes (2006) distinguen entre: 1) C2 aplicado a una organización —es decir, crear o transformar una organización o una asociación de organizaciones para adecuarla a sus desafíos y a las misiones a las que se enfrenta—, y 2) C2 aplicado a una tarea en específico. Esta dicotomía de creación de organización versus actividad permite, según Alberts y Hayes (2006), enfocarse en las funciones esenciales involucradas y un conjunto de métricas que es apropiado para la naturaleza del esfuerzo. Por lo tanto, las siguientes

7 De acuerdo con Álvarez y Jiménez (2021), el Comando y Control (C2) es un "conjunto de atributos y procesos organizativos y técnicos que emplea recursos humanos, físicos y de información para resolver problemas y lograr los objetivos de una organización o una misión" (p. 79). Por su parte el C3 incluye Comando, Control y Comunicaciones, y el C3I o el C4 abarcan el Comando, el Control, las Comunicaciones y la Inteligencia.

son funciones esenciales del C2: 1) establecer la comunicación necesaria para permitir el flujo de información y garantizar un entendimiento apropiado de la intención del comandante; 2) determinar roles, responsabilidades y relaciones; 3) establecer reglas y restricciones (horarios, etc.); 4) seguimiento y evaluación de la situación y de su progreso; 5) asignar recursos (información, personal y material); 6) entrenamiento y educación, y 7) abastecimiento.Con el desarrollo de nuevas amenazas, escenarios de combate y tecnologías, se generaron propuestas de nuevos modelos que describieran las nuevas exigencias del C2, basadas, en su mayoría, en la teoría del ciclo *observar, orientar, decidir, actuar* (OODA), desarrollado por el Coronel John Boyd, de la Fuerza Aérea de los Estados Unidos (USAF). Este es un modelo de proceso[8] que describe el C2 desde una perspectiva individual, como un proceso de decisión con retroalimentación e iteración. Fue desarrollado originalmente intentando explicar por qué los pilotos de aviones caza estadounidenses fueron más exitosos que sus adversarios durante la guerra de Corea (1950-1953).Como lo señala la sigla OODA, la primera actividad es *observar*, e involucra notar alguna característica del ambiente, y que en la primera versión del ciclo implicaba la detección de la aeronave enemiga. *Orientar* se refiere a apuntar u orientar la aeronave propia hacia la del enemigo, con el fin de obtener una buena posición respecto a ella y dar paso a la fase *decidir*, en la cual se establece lo que se va a hacer, para, finalmente, en la fase *actuar*, llevar a cabo lo decidido, como por ejemplo, disparar[9]. Luego de la fase de actuar, se hace una nueva observación, y así sucesivamente, el ciclo se repite, y termina cuando, simplemente, no haya nada más que observar, por falta de *inputs* (Boyd, 2018).

Complejidad de las operaciones multidominio con base en el C2

Al igual que el ciclo OODA de Boyd (2018), Carlisle (2019) considera que las FF. MM. en el siglo XXI pueden abordar los desafíos del C2 a través de tres capas de ejecución de operaciones. Primero está la capa de *detección* (inteligencia, vigilancia, reconocimiento y análisis), para comprender al enemigo, el medio ambiente y el lugar de los militares en la lucha conjunta de múltiples dominios. La

8 Boyd (2018) divide la cognición humana en cuatro procesos. El primero es la percepción (observación). El segundo es un pensamiento inconsciente denominado "orientación". El tercero es un acto consciente denominado "decisión". El cuarto es un comportamiento denominado "acción".

9 Cabe mencionar que Boyd (2018) extrapoló posteriormente el "orientar" de su representación de orientación física a representar la orientación mental, que se ve afectada por múltiples factores, dentro de los cuales introdujo: la herencia genética, las tradiciones culturales y las experiencias previas, así como el proceso mental de análisis y síntesis, e introduciendo algunos ciclos de retroalimentación.

segunda es la capa de C2. Y por último se encuentra la capa de *efectos*, la cual incluye operaciones cinéticas, no cinéticas y de información[10]. En consecuencia, para llevar a cabo operaciones multidominio se hace necesario mirar todos los dominios en relación con las tres capas.

En este sentido, el primer desafío por superar es la visualización, pues hay que ver cómo se relacionan los dominios entre sí. De acuerdo con Carlisle (2019), "¿se puede crear una imagen operativa común de todos los dominios, junto con las redes necesarias, para proporcionar a la fuerza conjunta toda la información necesaria para permanecer dentro del circuito OODA del adversario?" (p. 34). El segundo desafío es el tiempo, debido a que cada dominio funciona en diferentes líneas de tiempo, y estas deben coordinarse para que se produzca el efecto correcto en el momento adecuado; por ejemplo, un buque de guerra navega aproximadamente a unos 30 nudos, los aviones de combate rompen la barrera del sonido y las operaciones cibernéticas se mueven a la velocidad de la luz. El tercer desafío es la superioridad cibernética y del espectro. Las FF. MM. de Colombia deben operar hoy en todo el espectro electromagnético[11] para mantener las redes y crear efectos en los dominios objetivo; y todo, mientras el enemigo intenta hacer lo mismo.

Para ilustrarlo, Carlisle (2019) expone un escenario táctico de un grupo de objetivos móviles fuertemente defendidos en la zona litoral de un país hostil, en el que las operaciones multidominio de las FF. MM. estadounidenses requerirían mejoras: primero se necesitaría una capa de detección para encontrar, fijar y rastrear los objetivos, y que el sigiloso F-22 puede proporcionar; dada la cantidad de

10 En el marco de las guerras de quinta generación (Álvarez et al., 2017), existen ciertas diferencias entre "guerra de información" y "operaciones de información". Las formas tradicionales de operaciones de información, también referidas como guerra de C2, abarcan todas las tácticas militares que utilizan la tecnología de las comunicaciones, entre las cuales se contemplan las operaciones psicológicas, la guerra electrónica y las operaciones cibernéticas. Según Álvarez y Jiménez (2021), el objetivo en la *guerra de C2* "es negar información al enemigo y así interrumpir sus capacidades militares de comando y control, mientras que de manera simultánea se toman precauciones para proteger las propias capacidades de C2" (p. 79).

11 El espectro electromagnético (EEM) es el rango de frecuencias de radiación electromagnética y sus respectivas longitudes de onda y energías fotónicas. Es un recurso natural limitado, al cual, por la importancia que reviste para el desarrollo de las telecomunicaciones, se le asigna un valor estratégico, político y económico; por tales razones, la Constitución colombiana lo declaró como un bien público inajenable e imprescriptible, según el artículo 75 de la Carta Magna de 1991. Y en el artículo 101 de esta se preceptúa que forman parte de Colombia "el espacio aéreo, el segmento de la órbita geoestacionaria, el espectro electromagnético y el espacio donde actúa, de conformidad con el derecho internacional o con las leyes colombianas a falta de normas internacionales" (Constitución Política de Colombia, 1991). Aunque hoy por hoy no es ampliamente aceptado, algunos autores también definen el EEM como un dominio.

objetivos y el largo alcance necesario para alcanzarlos, se requeriría un submarino sigiloso capaz de penetrar las defensas enemigas el tiempo suficiente para cumplir la misión de alcanzar los objetivos en tierra con misiles *Tomahawk* de largo alcance. También se requiere una red para tomar los datos del sensor F-22 y enviarlos a los *Tomahawks*; una red de C2 crea una imagen operativa común del entorno, que permite al comandante de la Fuerza conjunta comprender lo que se necesita para llevar tanto al submarino como a los F-22 al lugar correcto, en el momento adecuado, para ejecutar la misión.

Pero el cumplimiento de la misión se vuelve más complejo a medida que se agregan otros requisitos de dominio; por ejemplo, es posible que se necesite un arma cibernética para interrumpir los sistemas integrados de defensa aérea del enemigo, y así permitir que los F-22 permanezcan en el espacio aéreo contiguo el tiempo suficiente para proporcionar información del sensor. Un equipo alfa del destacamento operativo de las Fuerzas Especiales puede estar en tierra tomando medidas para interrumpir la red de C2 del enemigo. Y es posible que sea necesario ajustar los satélites de comunicaciones y del sistema de posicionamiento global GPS, para que funcionen en un entorno de fuerte interferencia electromagnética. Como lo señala Parkinson (2019), durante la guerra de Yom Kippur (1973), Israel perdió una gran cantidad de aviones a manos de las defensas aéreas egipcias durante los primeros días del conflicto, ya que no pudo montar misiones de supresión de defensas aéreas enemigas (SDAE) contra los sistemas de misiles tierra-aire SA-6 egipcios, pues los receptores de alerta de radar de la Fuerza Aérea de Israel (FAI) no se programaron inicialmente para detectar el radar SA-6. Por ende, la FAI aprendió la importante lección de que la guerra electrónica había alcanzado la mayoría de edad.

Este aprendizaje fue puesto en práctica en un ejemplo moderno del uso de capacidades multidominio por parte de Israel, el 6 de septiembre de 2007. En efecto, la Operación Huerto fue un ataque aéreo ejecutado por Israel sobre una aparente central nuclear siria en Al-Kibar. Fue llevado a cabo por el 69.º Escuadrón de F-15 *Strike Eagle*, de la FAI, además de aviones F-16 *Fighting Falcon* y una aeronave de inteligencia electrónica israelí. Los aviones de combate estaban equipados con misiles aire-tierra AGM-65 *Maverick*, bombas de 227 kg y tanques externos de combustible. También participó un comando de *Shaldag*, o de la Unidad 5101: una unidad de comando de élite de la FAI, y quienes llegaron al lugar el día previo, para señalizar los objetivos vía láser. Los israelíes utilizaron durante la operación un sistema tecnológico similar al *Suter*, desarrollado por

Estados Unidos. Con dicho sistema, la FAI fue capaz de penetrar con sus aviones de combate en el espacio aéreo sirio sin ser detectados por radar. El sistema permitió manipular directamente la señal recibida por los radares enemigos, al mostrar en sus sensores objetivos falsos. Eso demostró la efectividad del sistema, dado que Siria disponía de dos sistemas modernos que había adquirido a Rusia poco tiempo antes de los ataques: los Tor-M1 y Péchora-2A.

No obstante, los sistemas integrados de defensa aérea se están volviendo cada vez más resistentes a la supresión electrónica mediante el uso de tecnologías de sensores pasivos, como la búsqueda y el seguimiento por infrarrojos. Dichos saltos tecnológicos se están incrementando con misiles tierra-aire que tienen un seguimiento avanzado y alcances más largos. Los adversarios potenciales también están invirtiendo en bloqueadores económicos de baja potencia a fin de inhibir el posicionamiento, la navegación y el tiempo necesarios para operaciones de ataque efectivas. Por ende, el panorama estratégico emergente del siglo XXI está revelando una amplia gama de nuevas amenazas.

De acuerdo con Reilly (2019), varios actores están aprovechando los avances tecnológicos para crear sus propias ventajas asimétricas: por ejemplo, Rusia, Irán, Corea del Norte y China han invertido en una serie de misiles de crucero balísticos y supersónicos, diseñados para desafiar la superioridad convencional de Estados Unidos y sus aliados[12]. Mientras tanto, Rusia, China y Estados Unidos trabajan en el desarrollo de misiles hipersónicos[13]; dichas armas vuelan muy rápido: por encima de Mach 5; es decir, al menos cinco veces la velocidad del sonido. Otros países están involucrados en el desarrollo y la producción de misiles de crucero de ataque terrestre, y muchas de tales armas ya están disponibles para la exportación. Las innovaciones en la tecnología de misiles de crucero han creado amenazas supersónicas que pueden atacar objetivos a 300 km de distancia y ser entregados por una variedad de sistemas como aviones, submarinos, barcos o, incluso, camiones.

Asimismo, los misiles de crucero modernos se pueden programar para

12 El DF-21D de China, un misil balístico de mediano alcance, tiene un vehículo de reentrada maniobrable, presenta una guía de terminal basada tanto en el GPS como en el radar activo, y puede atacar de 1.500 a 2.000 km de las costas de China.

13 El primer regimiento ruso de misiles hipersónicos Avangard ya se puso en servicio. Estos misiles, con capacidad nuclear, pueden viajar a más de 20 veces la velocidad del sonido y alcanzar un objetivo a 6.000 km. Montado sobre un misil balístico intercontinental, el Avangard puede transportar un arma nuclear de hasta 2 megatones. Tiene un "sistema de deslizamiento" que ofrece una gran maniobrabilidad y podría hacer que sea imposible defenderse de ellos.

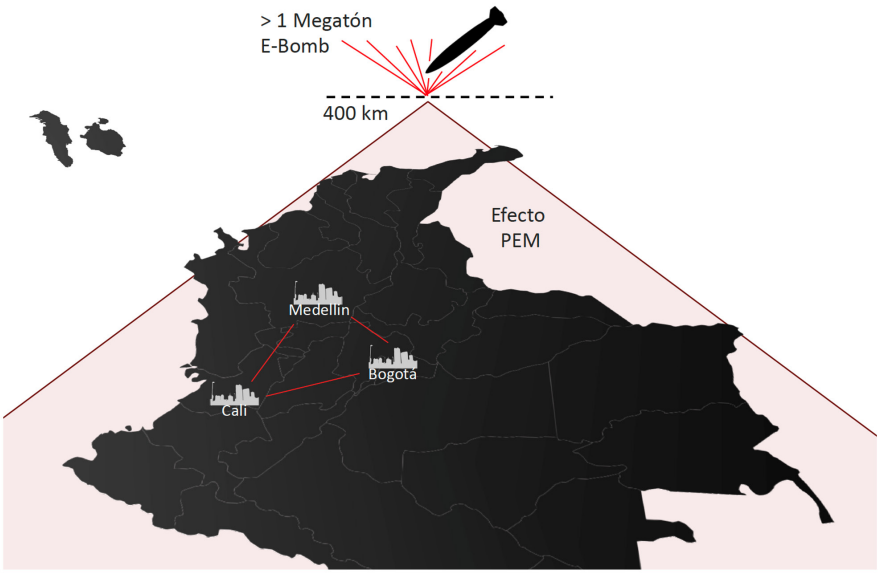
acercarse y atacar a un objetivo de la manera más eficiente, al permitir que un adversario dispare múltiples misiles y ataque simultáneamente desde diferentes direcciones, y así abrume las defensas aéreas en sus puntos más débiles[14]. Además de las amenazas de la tecnología avanzada de misiles, numerosos países vienen adquiriendo o desarrollando por sí mismos diferentes tipos de VART; muchos de esos países buscan mejorar no solo su adquisición de inteligencia, sino también, sus capacidades de ataque armado. De manera similar, numerosos países están trabajando en armas de microondas de alta potencia (MAP), energía dirigida y pulso electromagnético (PEM). Los PEM afectan los circuitos eléctricos y electrónicos no endurecidos, al generar una sobretensión en la corriente y el voltaje más allá de la capacidad de funcionamiento normal; por ejemplo, una explosión nuclear de un megatón detonada a 400 km de la superficie terrestre sobre el triángulo de oro de Colombia puede tener, en segundos, efectos sobre todos los dominios del país[15], como se muestra en la figura 2.

En definitiva, el entorno operacional del mundo posmoderno se compondría de factores y condiciones distintas de los del siglo XX, y los cuales deben entenderse para aplicar con éxito las capacidades militares, proteger la Fuerza y completar cualquier tarea. El entorno operacional se extiende más allá de los límites físicos de un área definida, pues incluye el mar, la tierra, el aire y el espacio, el enemigo, los actores neutrales, los aliados, las instalaciones, el clima, el terreno, el entorno de información, el EEM, y las amenazas y los peligros químicos, biológicos, radiológicos y nucleares (QBRN) (Parkinson, 2019). La mayoría de los factores que se combinan para crear el entorno operativo, si no todos, afectan a todos los dominios y, por lo tanto, a todos los componentes militares; un modelo gráfico para entender los dominios actuales y su relación se muestra en la figura 3.

14 Los misiles más nuevos están incorporando características de sigilo para hacerlos aún menos visibles para los radares y los detectores infrarrojos, y pueden armarse con ojivas nucleares convencionales, de combustible de aire o, incluso, de bajo rendimiento.

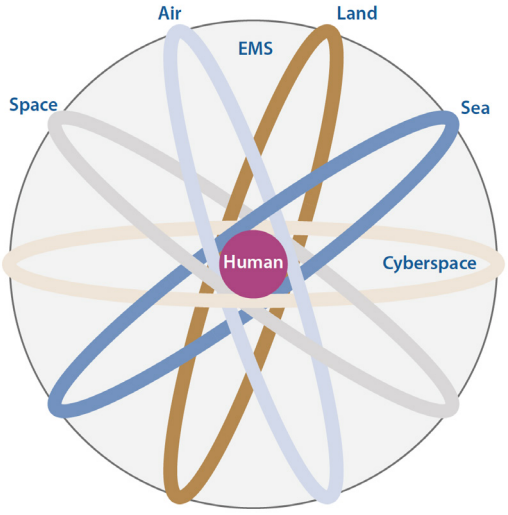
15 La prueba nuclear de 1962 "Starfish Prime", de Estados Unidos, demostró esa capacidad cuando un arma de 1.4 megatones fue detonada a 400 km sobre la superficie de la Tierra. Los efectos electromagnéticos de la detonación no solo abarcaron el conjunto del suelo continental de los Estados Unidos y de Hawái, sino que también crearon un intenso cinturón de radiación artificial que comenzó a dañar los satélites meteorológicos y de comunicaciones en órbita. El cinturón de radiación artificial destruyó siete satélites y persistió hasta principios de la década de 1970; para ponerlo en perspectiva, más del 40 % de los satélites activos del mundo están en órbita terrestre baja (Poveda & Álvarez, 2019).

Figura 2. *Un ataque PEM sobre Colombia.*



Fuente: elaboración propia.

Figura 3. *Continuum de dominios.*



Fuente: Parkinson (2019).

Poder multidominio: convergencia de los dominios aéreo, espacial y ciberespacial

Como se ha podido observar hasta el momento, la guerra siempre se ha constituido en un catalizador para el cambio y la adaptación militar; y la historia de las FF. MM. de Colombia no ha sido la excepción. De acuerdo con Davis y Arnott (2016), la guerra entre Colombia y Perú (1932-1933) demuestra perfectamente la forma como la necesidad militar —a menudo, bajo la apariencia de reveses o derrotas inesperadas— impulsa el desarrollo de capacidades. En 1932, aprovechando que Colombia tenía pocas posibilidades de defenderse, debido a la inaccesibilidad de la Amazonía colombiana y a la falta de una Fuerza Aérea y una Armada (la cual se había disuelto en 1909), Perú invadió territorio colombiano con dos regimientos de su ejército enviados a Leticia y Tarapacá. Pero la reacción colombiana fue inmediata, y en 90 días logró ubicar buques de guerra en la desembocadura del Amazonas, mientras que la pequeña flota de aviación militar, de cinco aviones, se expandió rápidamente, con la compra de 74 aviones adicionales y el préstamo de pilotos y aviones a la Sociedad Colombo-Alemana de Transportes Aéreos (SCADTA). Si bien el conflicto fue finalmente resuelto por la Liga de Naciones, como resultado, recrearía a la Armada y fortalecería las capacidades de la FAC, con la construcción de las bases aéreas de Madrid, Palanquero y Tres Esquinas.

Posteriormente, y en el inicio del conflicto armado interno, en la década de 1960, las FF. AA. de Colombia estaban diseñadas para proteger al país de las amenazas externas; pero ante la creciente expansión de fuerzas y la presencia guerrillera en la geografía nacional, desde principios de ese mismo decenio hasta finales del de 1990, hubo una serie de cambios incrementales en el Ejército Nacional (EJC), la Armada (ARC) y la FAC, así como en la Policía Nacional (PONAL). Pero los graves reveses tácticos de 1997 y 1998 convencieron al Gobierno y al liderazgo de las FF. AA. de que se necesitaba un cambio más radical para modernizar y fortalecer tanto a las FF. MM. como a la PONAL (Davis & Arnott, 2016). Este cambio fue impulsado por una nueva visión de cómo se debían realizar las operaciones contraguerrilleras combinando poder aéreo e inteligencia técnica y humana, así como mediante el uso de Fuerzas Especiales, en complejas operaciones conjuntas que involucraban al EJC, la ARC la FAC y la PONAL.

A principios de la década de 1990, la FAC era una organización relativamente pequeña, que contenía solo el 8 % del personal militar colombiano, y sus roles se enfocaron, en gran medida, en las amenazas externas; por lo tanto, su pilar para dicha tarea eran los Kfir israelíes y los Mirage-5 franceses, armados con misiles aire-aire *Python*. Asimismo, la FAC tenía una capacidad limitada de helicópteros, en la forma de una flota mixta de Bell UH-1 *Huey* (menos de 20) y un puñado de Hughes 500. Sin embargo, a fines de la década de 1990, la FAC no solo había crecido, sino que había adaptado sus capacidades para enfrentar las amenazas, cada vez más críticas, de la guerra de guerrillas y la lucha contra el narcotráfico[16].

En consecuencia, Esquivel (2017) explica que entre 1998 y 2015, la FAC lideró las operaciones decisivas que permitieron acercarse al cese del conflicto interno en contra de las insurgencias[17], como lo testifican las operaciones Vuelo de Ángel (1998) y Delta (2002), al igual las operaciones conjuntas y de bombardeo de precisión, como las operaciones Universal (2007), Aromo (2007), Sol Naciente (2007), Alcatraz (2007), Fénix (2008), Gibraltar (2008), Oriente (2009), Baltazar (2010), Fortaleza II (2010), Sodoma (2010), Odiseo (2011), Armagedón (2012), Elipsis (2013) y Darién (2013), entre otras.

El punto de inflexión inició, probablemente, en 1998, con la Operación Vuelo de Ángel, luego de la violenta toma de Mitú, capital del departamento del Vaupés, por parte de las FARC-EP. Sin otros aeródromos, y a menos de 400 km, una fuerza mixta de UH-60 *Blackhawks*, dos aviones fantasma AC-47 y dos aviones de transporte C-130 colombianos aterrizaron en la pista aérea brasilera Querarí, al otro lado de la frontera. Operando desde este puente aéreo temporal, la FAC inició operaciones alrededor de Mitú; los AC-47 (C-47 *Skytrains* mejorados, con autonomía de vuelo de 6 horas) proporcionaron inteligencia de lo que estaba sucediendo en las calles de Mitú, así como apoyo de fuego desde el aire con ametralladoras calibre 0.50. Gracias a la inteligencia y al apoyo de fuego de la FAC, se logró movilizar más de 300 soldados que, en los siguientes días, lograron no solo retomar Mitú, sino ocasionarle

16 Colombia ahora tiene una de las flotas de helicópteros más grandes del mundo (320), junto con aviones de ala fija (265), refinados para operaciones de precisión y tareas de vigilancia.

17 Según Esquivel (2017), la FAC inició su cuarto momento histórico a partir de 1998. Los cuatro momentos han sido: 1) la instauración, en 1916, que alcanza hasta la proyección del poder aéreo sobre Leticia, en 1932; 2) el decreto, en 1942, de autonomía operativa, bajo el nombre de la Fuerza Aérea Nacional; 3) la adquisición, en 1969, de la flotilla de helicópteros UH-1H, y en 1970, de aviones Mirage-5. y 4) la nueva proyección del poder aéreo, desde 1998.

graves bajas a la guerrilla de las FARC-EP; por ende, dicho evento anunciaba que el poder aéreo iba a jugar un papel clave en la derrota de las guerrillas (Davis & Arnott, 2016).

De acuerdo con Esquivel (2017), el bombardeo de precisión permitió no solo recuperar la zona de distención en un corto periodo, en 2002, sino también, debilitar las estructuras de mando de la guerrilla, al dar de baja, mediante este tipo de operaciones, a los principales cabecillas de las FARC-EP; entre 2010 y 2015, fueron neutralizados más de 60 cabecillas de diferentes niveles. Cono lo afirman Davis y Arnott (2016), esto fue posible gracias a la adquisición de nuevas aeronaves, municiones guiadas con precisión, e inteligencia y navegación avanzadas, proveídas por activos espaciales. Las primeras versiones del turbohélice de ataque ligero A-29 *Super Tucano* arrojan bombas guiadas Mk 82 sobre un área de 10 m2; versiones posteriores del A-29 estaban equipadas con telémetros láser, que resultaron esenciales en el uso temprano de las bombas guiadas por láser *Paywave* II, entregadas por los *Dragonfly* A-37[18]. Aunque Colombia adquirió su primer UH-60 *Black Hawk* en 1989, no fue sino hasta 1995 cuando nació la variante *Arpía*[19]. La última versión es el *Arpía 4*, equipado con cohetes, ametralladoras y el misil antitanque *Spike*[20]. También cuenta con dos minicañones de 20 mm, para brindar mayor potencia de fuego; especialmente, cuando la aeronave se aleja del objetivo.

En ese orden de ideas, el poder aéreo de la FAC desempeñó un papel central para que las operaciones conjuntas fueran exitosas[21]. Cada una de las transformaciones tecnológicas del poder aéreo, la inteligencia y las operaciones especiales fueron clave en la ofensiva militar del Estado colombiano en contra de los grupos al margen de la ley. Pero más importante fue la convergencia simultánea de estas capacidades, propias o delegadas; particularmente, de la sinergia de

18 En 2006, Colombia adquirió de Estados Unidos el GBU-12 *Paveway* II: una bomba MK 82 de 500 lb, de uso general y con un paquete de guía adicional que la convierte en un arma guiada por láser.

19 Llamado así por el águila arpía, de América del Sur (conocida por cazar monos).

20 El misil israelí *Spike* puede lanzarse desde una distancia de 24 km de su objetivo; es guiado por GPS, y en las últimas etapas del vuelo del misil, la tripulación del Arpía tiene la capacidad de ajustar el vuelo del misil hacia un objetivo en específico.

21 Probablemente, la inherente naturaleza conjunta del poder aéreo podría ser una de las principales razones de tal éxito (Canovas, 2019); de hecho, el componente aéreo (no siempre considerado únicamente dentro de una Fuerza Aérea), influye de forma rutinaria en los demás dominios.

los poderes aéreo[22], espacial[23] y ciberespacial[24] de la FAC. Por ejemplo, como lo señalan Zuluaga et al. (2020), sin el uso de satélites de posicionamiento, tiempo y navegación (PTN), los operadores militares colombianos no podrían "comunicarse entre sí ni aprovechar los sistemas militares avanzados, ya que son críticos para las capacidades de C2, comunicaciones y sistemas de información de la Fuerza Pública, lo que las hace indispensables para cualquier operación militar" (p. 284). Por eso, es imperativo que los dominios cibernéticos y espaciales deban defenderse para ejercer control en otros dominios.

> Los aviones Kfir C-10, A-29 Súper Tucano y A-37 Dragonfly de la FAC se basan en señales PTN para "navegar en los espacios aéreos y atacar objetivos con precisión, mediante sistemas de armas que hacen uso de señales GPS para fijar un conjunto de coordenadas geográficas definidas para una misión. Las fragatas de la Armada de Colombia también dependen en gran medida de se ales PTN, ya que los buques las utilizan para navegar los océanos y poseen una cantidad de sistemas de armas que no podrían funcionar sin ellas. (Zuluaga et al., 2020, p. 285)

Pero el cambiante entorno de la seguridad multidimensional de Colombia requiere que se examine cómo la FAC percibe, decide y actúa de forma rápida y concertada en todos los dominios, ya que potenciales adversarios de Colombia están combinando avances en tecnología con conceptos operativos y estrategias diseñadas para negar la maniobra militar colombiana en múltiples dominios. Si bien hoy la FAC domina el aire, el espacio y el dominio cibernético —al menos, en relación con los actores no estatales al margen de la ley—, los

22 Según el Manual de Doctrina Básica Aérea, Espacial y Ciberespacial (DBAEC) de la FAC, el poder aéreo es "un conjunto de capacidades aéreas, y la voluntad de emplearlas con el objeto de brindar seguridad y defensa a la nación y la consecución de los fines del Estado. El poder aéreo involucra la utilización y aplicación de los componentes de capacidad —DOMPI— para el logro de los objetivos impuestos por el nivel más alto de la política nacional. Dicho poder actúa de manera autónoma o en concierto, tanto con los poderes tradicionales como son el terrestre y el naval, como con los nuevos poderes, como son el espacial y el ciberespacial" (FAC, 2020a, 5-2).

23 De acuerdo con Álvarez, Murillo y Hernández (2019), el poder espacial es "la facultad y voluntad del uso de las capacidades espaciales de carácter civil, militar y sus infraestructuras asociadas, en apoyo de las estrategias de seguridad y desarrollo nacionales, así como del logro de los intereses nacionales objetivos y subjetivos" (p. 50). De acuerdo al DBAEC, y desde el punto de vista militar, el poder espacial es "la capacidad de emplear defensiva u ofensivamente la totalidad de las capacidades espaciales en favor de los fines del Estado. Para ello, el poder espacial actúa en concierto con los poderes militares de los otros dominios como el terrestre, naval, a reo y ciberespacial" (FAC, 2020a, 6-2).

24 Según el DBAEC, el poder ciberespacial se define como "la capacidad virtual de aplicar, controlar y aprovechar el ciberespacio para contribuir, a través de efectos en este y otros dominios" (FAC, 2020a, 7-1).

adversarios vienen invirtiendo en tecnologías que buscan negarle la superioridad a la FAC: por ejemplo, incursionando activamente en el dominio ciberespacial o haciendo uso con mayor entusiasmo de los VART para el espionaje, o incluso, ataques terroristas a las bases aéreas. Para contrarrestar esas y otras acciones de actores Estatales y no estatales, la FAC necesita integrar sus ventajas en dichos dominios, de una manera nueva y dramáticamente efectiva; o sea, unir aquellas operaciones que se mueven a la velocidad de la luz con las operaciones que se mueven a la velocidad del sonido.

Por ejemplo, la República Popular de China (RPC) está actualmente combinando lo que se conoce como tecnología *shashoujian* (carta de triunfo, o maza de asesino) con el concepto *guerra sin restricciones* y una estrategia de guerra de información. Estos son elementos clave en la guerra de quinta generación, y han sido incorporados por varios países, como es el caso de Venezuela. *Shashoujian* se refiere a un conjunto de capacidades militares que permite a los tecnológicamente inferiores derrotar a los tecnológicamente superiores. Estas capacidades incluyen sistemas avanzados integrados de defensa aérea, misiles balísticos y de crucero, aviones de ataque avanzados, submarinos de ataque y capacidades antisatélite. La estrategia de guerra sin restricciones aboga por ir más allá de los límites tradicionales de la guerra, cuando sea necesario, para lograr los objetivos políticos nacionales. Proponen el uso de ataques *shashoujian* en los nodos críticos de un adversario superior, a fin de paralizar sus fuerzas y causar la desintegración de estas.

El siguiente extracto del libro *Guerra sin Restricciones*, de los coroneles Qiao Liang y Wang Xiangsui, proporciona una visión excepcionalmente aleccionadora sobre los fundamentos conceptuales de *shashoujian* y el concepto de guerra sin restricciones:

> Suponiendo que estallara una guerra entre dos Estados que ya poseen tecnología de información completa, y confiando en los métodos tradicionales de operación, el lado atacante generalmente emplearía los modos de gran profundidad, frente amplio, alta resistencia y tridimensionalidad para lanzar un ataque de campaña contra el enemigo [...] Sin embargo, al usar un método combinado, puede ocurrir un escenario y juego completamente distinto: si el lado atacante reúne secretamente grandes cantidades de capital sin que el Estado enemigo se dé cuenta de ello, y lanza un ataque furtivo contra sus mercados financieros e inserta anticipadamente un virus informático en el sistema informático del oponente, al mismo tiempo que realiza un ataque de red contra el adversario, para que la infraestructura de electricidad civil, la red

> de tráfico aéreo y terrestre, la red de transacciones financieras, la red de comunicaciones telefónicas y la red de medios de comunicación están completamente paralizados, esto hará que el Estado enemigo se vuelva una víctima del pánico social, los disturbios callejeros y una crisis política. Finalmente, los medios militares se utilizan en etapas graduales hasta que el enemigo se ve obligado a firmar un tratado de paz deshonroso. (Liang & Xiangsui, 1999, pp. 145-146)

La Unidad 61398 del Ejército Popular de Liberación (EPL) destaca la capacidad y la voluntad de China para llevar a cabo operaciones de explotación y ataque cibernético a escala mundial. Las capacidades cibernéticas de China van mucho más allá de la recolección y la explotación de datos de inteligencia. El EPL está creando activamente las herramientas, el personal capacitado y la orientación estratégica necesarios para emplear las operaciones de red informática en apoyo de los dominios tradicionales de guerra. El ciberespacio ofrece a China y otros actores estatales y no estatales la capacidad para retrasar la respuesta de un adversario a un ataque cinético, mediante la implantación anticipada de códigos maliciosos en la logística del enemigo; en su comando, su control, sus comunicaciones, sus computadores, su inteligencia, su vigilancia y su reconocimiento, así como en sus redes de apoyo comercial e industrial.

Las evaluaciones del EPL de conflictos actuales y futuros indican que las campañas se llevarán a cabo de manera simultánea en todos los dominios, si bien su énfasis en el espectro electromagnético lo ha llevado a adoptar un enfoque mucho más integral. China considera la guerra electrónica un poder intangible necesario para el éxito, pues cualquier actor que pierda en una guerra electrónica se "reducirá a la ceguera y la sordera", por lo cual sus armas se desactivarán y perderá su iniciativa en una batalla, en una campaña militar o en un contexto estratégico más amplio. La doctrina militar del EPL enfatiza que el dominio electromagnético en las primeras fases de una campaña es una de las principales tareas para garantizar el éxito en el campo de batalla; dicha estrategia, conocida como *guerra electrónica de red integrada*, combina la guerra electrónica, las operaciones de la red informática y los ataques cinéticos para interrumpir los sistemas de información en el campo de batalla que respaldan las capacidades de combate de guerra y proyección de poder de un adversario.

Este tipo de guerra también enfatiza que el espectro electromagnético es una cuarta dimensión vital, tan importante como las fuerzas terrestres, marítimas y

aéreas tradicionales. Por consiguiente, la nueva estrategia militar de China es un presagio de una tendencia más amplia, en la que actores estatales menos poderosos, como Venezuela, e incluso, actores no estatales, buscan desarrollar o adquirir capacidades asimétricas que están cambiando la noción tradicional de las operaciones militares. La estrategia de guerra venezolana ahora combina capacidades convencionales y no convencionales, así como la estrategia de guerra de información. Combina capacidades convencionales de sistemas integrados de defensa aérea, aviones de ataque avanzados, tanques y artillería, destructores navales y capacidades satelitales de observación, junto con capacidades no convencionales, como colectivos armados y la Fuerza Armada Nacional Bolivariana, para la "guerra popular prolongada" (Álvarez et al., 2017), al igual que el uso del Servicio Bolivariano de Inteligencia Nacional (SEBIN) y el G-2 cubano, para la guerra de información.

Para Colombia, las implicaciones de este fenómeno son numerosas y lo suficientemente graves como para exigir una nueva mirada a cómo educamos a los futuros líderes de la FAC para desarrollar, coordinar y ejecutar operaciones aéreas, espaciales y ciberespaciales. Ya no es suficiente con que la FAC sea "dueña" del aire, pues si bien este es el dominio donde la FAC tradicionalmente ha proyectado su poder, para ser efectiva en el siglo XXI la FAC debe adquirir la maestría, tanto intelectual como física, del dominio espacial y el ciberespacial. En consecuencia, los autores de este capítulo consideran que para construir dicha maestría sería útil afianzar el concepto de poder multidominio dentro del pensamiento estratégico y la doctrina de la FAC. Si se parte de la generalidad de que un dominio es la esfera de conocimiento, influencia o actividad, los autores del presente capítulo proponen que una definición inicial del poder multidominio sería, por lo tanto,

> […] la capacidad y voluntad de emplear de manera convergente los activos aéreos, espaciales y ciberespaciales de la FAC, con el objeto de contribuir a la misión de la institución, al apoyo de los otros dominios de tierra y mar, así como a la satisfacción de los intereses nacionales de Colombia.

Este concepto es un aporte al pensamiento estratégico aéreo, espacial y ciberespacial de la FAC, y se inscribe dentro del metaconcepto del *poder aéreo, espacial y ciberespacial* (PAEC), puesto en conocimiento de los miembros de la FAC y del público colombiano en la quinta edición del Manual de Doctrina Básica Aérea, Espacial y Ciberespacial (DBAEC), de la FAC, de 2020. En el DBAEC aparece 69 veces el término "PAEC", y nueve veces, el término "PAEC integrado", lo

que lleva a inferir un uso independiente o integrado del PAEC. Al referirse al PAEC integrado, la FAC (2020a) señala:

> Con la integración de los dominios aéreo, espacial y ciberespacial, la FAC se convierte en un sistema integrado vital para la defensa de la nación. A la combinación de los efectos físicos logrados desde el aire y el espacio, se suma la posibilidad de alcanzar los fines establecidos por la estrategia a través de acciones no cinéticas desde el ciberespacio. Esta triple alternativa facilita las operaciones en cualquier dominio con varias posibilidades de cursos de acción y enormes ventajas para el poder militar. En un teatro de guerra u operaciones, la sinergia total se logra cuando el PAEC se emplea sin segregaciones buscando el mismo efecto. Por ejemplo, la inteligencia técnica desde satélites se complementa con las hechas desde plataformas aéreas, redes de inteligencia y el ciberespacio; estas interacciones potencializan la calidad de la información y reducen los márgenes de error de la alerta situacional del campo de batalla. (FAC, 2020a, 8-1)

Entonces, el poder multidominio no debería interpretarse como un concepto que entre en conflicto con el PAEC o con el concepto de operaciones multidominio; como ya se ha mencionado, las operaciones multidominio aluden a la integración de los cinco dominios (tierra, mar, aire, espacio y ciberespacio), mientras que el PAEC integrado se acerca a la definición anteriormente propuesta del "poder multidominio", pero no es exactamente lo mismo. Si se entiende al poder multidominio como la capacidad y voluntad de emplear de manera convergente los activos aéreos, espaciales y ciberespaciales de la FAC, por su esencia, implica, necesariamente, el uso integrado de dichas capacidades, y no de manera independiente, fomentando el pensamiento de MDC-2.

El MDC-2 puede definirse como "la ejecución coordinada de autoridad y dirección para obtener, fusionar y explotar información de cualquier fuente para integrar la planificación y sincronizar la ejecución de operaciones multidominio en tiempo, espacio y propósito para cumplir los objetivos del comandante" (Canovas, 2019, p. 49). Según Zadalis (2018), el MDC-2 es la habilidad para analizar, fusionar y compartir de forma continua lo que una vez fue información centralizada por dominios, en un sistema de C2 que soporte todos los dominios y los niveles de la guerra (estratégico, operativo y táctico); es decir, información rápidamente analizada, integrada y diseminada.

Para mayor claridad sobre el concepto de MDC-2, Goldfein (2018) hace una analogía con el fútbol. Goldfein (2018) parte del supuesto de que el equipo A ha

conformado y empleado la mejor delantera de ataque que el deporte del fútbol haya visto jamás. Pero con el tiempo, los equipos B y C ajustaron y construyeron sus defensas para limitar la efectividad de la delantera del equipo A. Por lo tanto, el equipo A se ve en la obligación de desarrollar un nuevo estilo de ataque; eso no implica abandonar la formación del equipo A, sino mejorar la efectividad de los pases y crear un ataque multidimensional que mantenga desequilibrada a la defensa rival (porque es posible atacarla de múltiples formas), y aumentando el ritmo y la intensidad del juego, para que el adversario no tenga tiempo de adaptarse o recuperarse.

Goldfein (2018) insiste en que debe abrumarse al rival, y esta evolución en las capacidades de comando y control del equipo A (sistema de juego) requiere una nueva idea de juego, nuevas rutinas de entrenamiento y, por supuesto, nuevas tecnologías (jugadores), o nuevas formas de utilizar la tecnología anterior (formación de juego[25]). Por lo tanto, el equipo A necesita integrar información en tiempo real de una variedad de todas las fuentes y evaluar esa información tan rápido como los sistemas puedan procesarla; si el equipo B o C bloquea acciones en un dominio, el equipo A debe cambiar rápidamente la táctica de juego, y atacar o defender desde otro dominio. Esto implica que las futuras operaciones multidominio serán ágiles y conjuntas, de alta velocidad, por su propia naturaleza.

La batalla multidominio es más que la capacidad para trabajar en múltiples dominios, y es más que las operaciones en un dominio que respaldan operaciones en otro dominio. Por consiguiente, un concepto operativo multidominio avanzado aprovechará las capacidades nuevas y actuales, además de integrar las capacidades conjuntas y de coalición en todas las operaciones militares; y esa responsabilidad exige la articulación del MDC-2 (Craider, 2018). Las acciones en un solo dominio influirán cada vez más en los demás, y así crearán ventanas de oportunidad para lograr resultados favorables, incluso en los dominios en disputa. Dado eso, se requerirá una estructura MDC-2 efectiva para reconocer ventanas de oportunidad, a través del conocimiento de la situación en tiempo real en todos los dominios, y ejecutar ciclos de decisión más rápidos. La FAC debe integrarse y colaborar estrechamente con la industria, para obtener una ventaja de las

25 Las formaciones en el fútbol son un método de posicionar jugadores en el campo para permitir que un equipo juegue según una táctica preestablecida; pueden usarse formaciones diferentes dependiendo de si la táctica va a ser más atacante o más defensiva. Las formaciones pueden alterarse durante el juego, pero esto requiere una adaptación de los jugadores para que se ajusten al nuevo sistema.

tecnologías emergentes y reducir los ciclos de adquisición; especialmente, en los campos de la AI y la ciberdefensa. Por último, se necesita un esfuerzo de capacitación para formar expertos en el poder multidominio, capaces de combinar los dominios aéreo, espacial y ciberespaciales en la planificación y la ejecución en el nivel operativo, desde las primeras etapas de su carrera militar.

Conclusiones

Los avances en la tecnología han empujado sutilmente a todas las FF. MM. estatales a un reino donde todas las nociones previas del espacio de batalla comienzan a ser reexaminadas —incluso, reinterpretadas—, y a crear, entonces, un entorno donde la falla en un dominio tiene efectos en cascada en uno o más de los otros. En tal sentido, la esencia de las operaciones multidominio es pensar en la resolución de problemas militares de manera no lineal, y realizar las operaciones centradas en lograr los objetivos, en vez de mantener líneas distintas entre los componentes militares. El pensamiento tradicional que alinea rígidamente los dominios y los componentes (la tierra con el Ejército, el marítimo con la Armada y el aire con la Fuerza Aérea) no será, por lo tanto, del todo eficaz en el futuro. La complejidad de las operaciones actuales y futuras requiere abandonar este patrón de pensamiento, para integrar más continuamente las capacidades únicas de cada componente, a fin de crear los efectos necesarios para lograr objetivos tácticos, operacionales y estratégicos.

Como lo ha demostrado la historia, ninguna institución armada lucha por sí sola, aunque cada una frecuentemente solía pensar y planificar de manera individual. Y el problema de planificación aislada ha ocurrido muchas veces en Colombia; por ende, para lograr el requerido nivel de cooperación institucional exigido por el planteamiento multidominio, el fundamento debe ser un entendimiento común de las operaciones multidominio, ya que, en la historia reciente de Colombia, las metodologías operacionales conjuntas han demostrado su eficacia en el combate, como lo testifican las Fuerzas de Tarea Conjuntas (FTC), que se crearon en el siglo XXI para enfrentar a las guerrillas en Colombia[26]. Y

26 En 2004, el Gobierno nacional formó la FTC "Omega", para coordinar los esfuerzos del EJC, la FAC y la Infantería de Marina en el centro de Colombia; Omega, la primera de trece operaciones de la FTC (Omega, Nudo de Paramillo, Sur del Tolima, Vulcano, Quirón, Apolo, Pegaso, Ares, Poseidón, Zeus, Titán, Algeciras y Hércules), permitió recuperar el control sobre una gran parte del territorio previamente ocupado por las FARC-EP en la región de La Macarena, y creó las condiciones necesarias para atacar a los líderes de esa organización subversiva.

aparte de la estructura doctrinal de la FTC que venido siendo utilizada durante los últimos 25 años para promover la capacidad conjunta, el desarrollo de las operaciones multidominio en Colombia ya se contempla en la planeación en los niveles de la estrategia nacional y la estrategia militar general, como se evidencia en el Plan Nacional de Desarrollo (DNP, 2018), la Política de Defensa y Seguridad (MinDefensa, 2019a), el Plan Estratégico Sectorial (MinDefensa, 2019b), el Plan Estratégico Militar (COGFM, 2018), el Plan Estratégico Institucional FAC (FAC, 2011), el Manual de Doctrina Básica Aérea, Espacial y Ciberespacial de la FAC (FAC, 2020a) y la Visión Futuro de las Fuerzas Armadas (MinDefensa, 2016).

Esto permitirá que las FF. MM. colombianas aprovechen el potencial de nuevos dominios emergentes, tales como el espacio y ciberespacio. En ese sentido, cobra validez la estrategia del control y poder multidominio de la FAC, o la facultad para actuar de forma conectada, combinada o reconfigurada en los dominios del aire, el espacio y el ciberespacio, en contra de amenazas convencionales o de orden no tradicional. Es probable que todos los conflictos futuros estén saturados, disputados y conectados a través de los medios y usando el ciberespacio. Esto sugiere que el dominio del espacio de la información será crítico para el éxito de las operaciones militares. Por su parte, el espacio exterior no se trata solo de vigilancia: también ofrece las funciones precisas de navegación y sincronización que sustentan cada una de las infraestructuras críticas del Estado (desde las transacciones financieras hasta el suministro de agua). Sin embargo, no ejercemos casi ninguna capacidad propia en ese dominio, y confiamos, en cambio, en nuestra capacidad para negociar el acceso que requerimos con nuestros aliados —en particular, Estados Unidos— y de fuentes comerciales.

Esta es una posición incómoda e insostenible para Colombia. En dicha construcción, el EEM potencia el espacio, lo que le permite suministrar habilitadores clave para los dominios del aire, la tierra y el mar, lo que, a su vez, facilita la capacidad para influir o controlar el dominio humano. Hipotéticamente, si un oponente ataca o manipula el uso de radiofrecuencias dentro del EEM, a través de medios cibernéticos u otros, podría negar el acceso a satélites vitales en los que el Estado colombiano confía para la inteligencia, la vigilancia, el reconocimiento, las comunicaciones, la advertencia temprana y la navegación. Es, por lo tanto, de suma importancia que los futuros oficiales de la FAC sean muy conscientes de este entorno operativo integrado, para garantizar que una superioridad local suficiente en la combinación correcta de dominios fomente las condiciones necesarias para el éxito operativo.

Con base en el poder multidominio, se busca lograr la unidad de mando o la unidad de esfuerzos, a través de la unidad de pensamiento conceptual. A raíz de ello, en la estrategia operacional de la FAC se debe usar un planteamiento de poder multidominio, con miras al apoyo de las misiones en tierra; un dominio que usualmente compromete el grueso del accionar de las FF. AA. colombianas en contra de los actores al margen de la ley en el contexto doméstico. La intersección de los dominios aéreo y terrestre abarca un gran número de conjuntos de misión, incluyendo: la movilidad aérea; el espacio; lo cibernético; la recuperación de personal; fuegos; inteligencia, vigilancia y observación, y muchos otros. La tecnología posmoderna está fusionando rápidamente un continuo de dominios integrados e interdependientes. Por ende, el poder multidominio o la convergencia entre el poder aéreo, espacial y ciberespacial representan la estrategia integral para la guerra posmoderna. Así lo exige la visión de la FAC:

> En el año 2042, la Fuerza Aérea Colombiana ejerce el dominio en el aire, espacio y ciberespacio, consolidándose como innovadora, polivalente, interoperable, líder y referente regional, con alcance global y con capacidades disuasivas reales, visibles, creíbles, permanentes y sostenibles. Se resalta su exitoso modelo de doctrina multidominio, consolidado con herramientas tecnológicas logrando obtener una doctrina ajustada, actualizada, ejercitada y con alta difusión, adaptada a los contextos emergentes en los que opera la Fuerza, toda vez que es capaz de influir en el entorno. (FAC, 2020b, 3-7)

Referencias

Alberts, D., & Hayes, R. (2006). *Understanding command and control*. DoD Command and Control Research Program.

Allen, P., & Gilbert, D. (2009). The information sphere domain: increasing understanding and cooperation. En C. Czosseck & K. Geers (Eds.), *The virtual battlefield: perspectives on cyber warfare* (pp. 132-142). IOS Press.

Álvarez, C., & Botero, D. (2021). Guerra y pestilencia: impacto de epidemias y opandemias en la historia hasta el siglo XX. *Revista Científica José María Córdova, 19*(35), 573-597.

Álvarez, C., & Jiménez, H. (2021). Guerra de información y ética militar: entre la tradición de guerra justa y la teoría de guerra irrestricta. En J. Jiménez, C. Figueroa & M. Bricknell (Eds.), *Ética militar y nuevas formas de guerra: retos para las Fuerzas Armadas de Colombia* (pp. 71-111). Sello editorial ESMIC.

Álvarez, C., & Ramírez, Y. (2020). La cuarta revolución y le era de la inteligencia artificial: implicaciones en la segurudad y el trabajo. En Y. Rico, D.López & A. Cerón (Eds.), Enfoques y gestión en seguridad integral (pp. 209-237). Escuela de Posgrados de la Fuerza Aérea Colombiana.

Álvarez, C., Benavides, E., & Ramírez, Y. (2019). Geopolítica del espacio exterior: dominio estratégico del siglo XXI para la seguridad y defensa. En C. Álvarez & C. Corredor (Eds.), *Mirando hacia las Estrellas: una constante necesidad humana* (pp. 85-193). Planeta.

Álvarez, C., Murillo, S., & Hernández, J. (2019). El poder espacial y la seguridad multidimensional. En C. Álvarez & C. Corredor (Eds.), *Mirando hacia las Estrellas: una constante necesidad humana* (pp. 22-83). Planeta.

Álvarez, C., Ramírez, Y., & Castaño, G. (2018). Geografía, Estado y gran estrategia. En C. Álvarez & A. Fernández (Eds.), *La "gran estrategia": instrumento para una política integral en seguridad y defensa* (pp. 81-148). Sello Editorial ESMIC.

Álvarez, C., Santafé, J., & Urbano, O. (2017). Metamorphosis bellum: ¿mutando a guerras de quinta generación? En C. Álvarez (Ed.), *Escenarios y desafíos de la seguridad multidimensional en Colombia* (pp. 145-248). Ediciones ESDEG.

Boyd, J. (2018). *A discourse on winning and losing*. Maxwell Air Force Base, Air University Press.

Bruce, J. (2006). *The pacific campaign in World War II: from Pearl Harbor to Guadalcanal*. Routledge.

Canovas, J. (2019). Multi-domain operations and challenges to air power. En *Shaping NATO for multi-domain operations of the future* (pp. 47-54). Joint Air Power Competence Center.

Carlisle, H. (2019). The complexity of multi-domain operations. En *Shaping NATO for multi-domain operations of the future* (pp. 33-37). Joint Air Power Competence Center.

CEDCO. (2018). *MFC 1-0 Doctrina Conjunta*. Comando General de las Fuerzas Militares.

Childs, T. (1990). *Italo-turkish diplomacy and the war over Libya 1911-1912*. E.J. Brill.

COGFM. (2018). *Plan Estratégico Militar PEM 2030*. Comando General Fuerzas Militares de Colombia.

Constitución Política de Colombia [Const.]. Julio 6 de 1991 (Colombia).

Craider, K. (2018). *Multi-domain command and control: proceedings of a workshop in brief*. The National Academies Press.

Davis, D., & Arnott, A. (2016). Building the tools for military success. En D. Davis, D. Kilcullen, G. Mills & D. Spencer (Eds.), *A great perhaps? Colombia: conflict and convergence* (pp. 45-60). Hurst and Company.

Departamento Nacional de Planeación (DNP). (2018). *Plan Nacional de Desarrollo 2018-2022: Pacto por Colombia/Pacto por la Equidad*. Departamento Nacional de Planeación.

Donnelly, J., & Farley, J. (2019). Defining the "domain" in multi-domain. En *Shaping NATO for multi-domain operations of the future* (pp. 5-16). Joint Air Power Competence Center.

Dorr, R. (2011). The air war. En C. Oldham (Ed.), *Desert shield/desert storm: The 20th anniversary of the Gulf War* (pp. 4-15). Faircount Media Group.

Esquivel, T. (2017). Fuerza Aérea Colombiana y operaciones decisivas 1998-2015. En E. Triana (Ed.), *Victorias desde el aire: la Fuerza Aérea Colombiana y el término del conflicto armado* (pp. 43-116). Editorial Ibáñez.

Fuerza Aérea Colombiana (FAC). (2011). *Plan Estratégico Institucional 2011-2030*. Fuerza Aérea Colombiana.

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

Fuerza Aérea Colombiana (FAC) (2020a). *DBAEC - Manual de doctrina básica aérea, espacial y ciberespacial*. Fuerza Aérea Colombiana.

Goldfein, D. (2018). *MDC2 Implementation Plan*. USAF Chief of Staff. https://n9.cl/mu1rc3

Grest, H., & Heren, H. (2019). What is a multi-domain operation? En *Shaping NATO for multi-domain operations of the future* (pp. 1-14). Joint Air Power Competence Center.

Heftye, E. (2017). *Multi-domain confusion: All domains are not created equal, en the strategy bridge*. https://n9.cl/itqom

Hoffman, F., & Davies, M. (2013). Joint Force 2020 and the Human Domain: Time for a New Conceptual Framework? *Small Wars Journal*. https://n9.cl/1t3a9

Krepinevich, A. (1992). The military-technical revolution: A preliminary assessment. Office of Net Assessment.

Liang, Q., & Xiangsui, W. (1999). *Unrestricted warfare*. PLA Literature and Arts Publishing House.

Ministerio de Defensa Nacional (MinDefensa) (2016). *Visión Futuro de las Fuerzas Armadas*. Imprenta Nacional de Colombia.

Ministerio de Defensa Nacional (MinDefensa). (2019a). *Política de defensa y seguridad PDS: Para la legalidad, el emprendimiento y la equidad*. Ministerio de Defensa Nacional.

Ministerio de Defensa Nacional (MinDefensa). (2019b). *Plan Estratégico Sectorial 2019-2022*. Ministerio de Defensa Nacional.

Parkinson, J. (2019). Is Fluidity the Key to Effective Multi-Domain Operations? En *Shaping NATO for multi-domain operations of the future* (pp.39-46). Joint Air Power Competence Center.

Poveda, A., & Álvarez, C. (2019). Colombia y la órbita geoestacionaria: un vínculo geoestratégico inalienable. En C. Álvarez & C. Corredor (Eds.), *El cielo no es el límite: el futuro estelar de Colombia* (pp. 85-188). Fuerza Aérea Colombiana.

Reilly, J. (2019). Multi-domain operations. En *Shaping NATO for multi-domain operations of the future* (pp.15-26). Joint Air Power Competence Center.

US Army TRADOC. (2018). *The U.S Army in multi-domain operations 2028*. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf

US Department of Defense. (2005). *Capstone Concept for Joint Operations V 2.0*. http://edocs.nps.edu/dodpubs/org/JROC/CCJO.pdf

USAF. (2015). *Air Force future operating concept - a view of the Air Force in 2035*. USAF Chief of Staff.

US Joint Force Development (2017). Joint Publication 5-0: Joint Planning. https://www.airforcespecialtactics.af.mil/Portals/80/prototype/assets/joint-pub-jpub-5-0-joint-planning.pdf

Weitz, R. (2004). Jointness and desert storm: a retrospective. *Defense & Security Analysis, 20*(2), 133-152.

Wells, H. G. (1902). *Anticipations: of the reaction of mechanical and scientific Progress upon human life*. Chapman & Hall.

Wells, H. G. (1908). *The war in the air and particularly how Mr. Bert Smallways fared while it lasted*. George Bell and Sons.

Zadalis, T. (2018). MDC2: Maintaining our asymmetric advantage, En *Shaping NATO for multi-domain operations of the future* (pp.23-42). Joint Air Power Competence Center.

Zuluaga, O., Aristizábal, H., & Sánchez, K. (2020). El acceso al espacio exterior como un interés nacional vital de Colombia. En E. Pastrana, S. Reith & F. Cabrera (Eds.), *Identidad e intereses nacionales de Colombia* (pp. 279-314). Fundación Konrad Adenauer/ Escuela Superior de Guerra.


EDITORIAL ESDEG

Poder aéreo, espacial y ciberespacial,

frente a desafíos y amenazas multidimensionales que afectan al Estado colombiano

Este libro contribuye en la construcción de nuevo conocimiento como respuesta a las preocupaciones que enfrenta el Estado Colombiano para enfrentar las amenazas multidimensionales que generan riesgos en sus intereses. Motivo por el cual, la nación colombiana está en la obligación de emplear lo mejor de las capacidades del poder aéreo, el poder ciberespacial y el poder espacial en ambientes multidominio, con el fin de contener y combatir dichas amenazas. Sin embargo, el incremento y la mutación de estas circunstancias de riesgo, mantiene al Estado colombiano en permanente alerta, para negar y/o disuadir estas amenazas multidimensionales.

La Escuela Superior de Guerra considera importante emplear este libro en todos los escenarios como un elemento de análisis, consciente de que lo consignado no se convierte en una limitante a la crítica o el debate, donde la argumentación y respeto por las ideas sean los pilares de la discusión.

EDITORIAL ESDEG

ESMIC
SELLO EDITORIAL

ISBN 978-628-7602-09-0