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.