Capítulo 4

Dominio ciberespacial en la Antártida: retos y oportunidades*

DOI: https://doi.org/10.25062/9786287602199.04

Gustavo Adolfo Salamanca Guzmán
Escuela Superior de Guerra "General Rafael Reyes Prieto"

Resumen: El presente capítulo identifica los retos y oportunidades que enfrenta el Estado colombiano en materia de dominio ciberespacial en la Antártida, dominio en el que nuestro país evidencia una falta de arquitectura de seguridad. Aunque el Tratado Antártico prohíbe la explotación de recursos y el desarrollo de operaciones militares, debe tenerse presente que el mundo contemporáneo se caracteriza por la volatilidad de las políticas exteriores de los países y el incremento de capacidades de los grupos al margen de la ley en materia de seguridad global. Por tal razón, la seguridad, en general, y la seguridad ciberespacial, en particular, cobran importancia vital en la protección de las labores humanas y las investigaciones científicas que se desarrollan en el Continente Blanco.

Palabras clave: capacidades; ciberespacio; ciberdefensa; ciberseguridad; retos; oportunidades.

* Capítulo de libro resultado del proyecto "La importancia de la Antártida para Colombia. Territorio de ciencia, protección del medioambiente y seguridad internacional", del grupo de investigación "Masa Crítica", de la Escuela Superior de Guerra "General Rafael Reyes Prieto", categorizado A1 por el Ministerio de Ciencia, Tecnología e Innovación (MinCiencias), código COL0123247. Los puntos de vista y los resultados de este capítulo pertenecen a los autores y no reflejan necesariamente los de las instituciones participantes.

Gustavo Adolfo Salamanca Guzmán
Mayor de la Fuerza Aérea Colombiana. Maestrando en Ciberdefensa y Ciberseguridad. Especialista en Sistemas de Gestión de la Calidad. Administrador aeronáutico, Escuela Militar de Aviación, Colombia. Ingeniero mecánico, Universidad de América, Colombia. Alumno Curso de Estado Mayor 2022. Operador de Aeronaves Remotamente Tripuladas. Contacto: **salamancag@esdeg.edu.co**

Citación APA: Salamanca Guzmán, G. (2023). Dominio ciberespacial en la Antártida: retos y oportunidades. En D. Barrero-Barrero y M. Tovar Zambrano (Eds.), *La importancia de la Antártida para Colombia: Vol. 1. Geopolítica, ciencia y global common* (pp. 107-141). Sello Editorial ESDEG. https://doi.org/10.25062/9786287602199.04

LA IMPORTANCIA DE LA ANTÁRTIDA PARA COLOMBIA:
Vol. 1. GEOPOLÍTICA, CIENCIA Y *GLOBAL COMMON*

ISBN impreso: 978-628-7602-15-1 (Obra completa)
ISBN digital: 978-628-7602-18-2 (Obra completa)
ISBN impreso: 978-628-7602-16-8
ISBN digital: 978-628-7602-19-9

DOI: https://doi.org/10.25062/9786287602199

Colección Derechos Humanos y DICA
Sello Editorial ESDEG
Escuela Superior de Guerra "General Rafael Reyes prieto"
Bogotá D.C., Colombia
2023

Introducción

Desde su descubrimiento, la Antártida representa una serie de oportunidades y desafíos de desarrollo, supervivencia y respuestas medioambientales para la humanidad. Por su tamaño y composición, es considerado el regulador del clima al sur del planeta, ya que posee el 70 % de las reservas mundiales de agua dulce. De allí que se afirme que el Polo Sur es un "amplio territorio con recursos minerales no contaminados y aptos para la investigación científica; además, cuenta con una gran cantidad de otros recursos naturales disponibles para la explotación" (Álvarez & Namen, 2019, p. 727).

Aunque el artículo 7 del Protocolo al Tratado Antártico Sobre Protección del Medioambiente establece que "Cualquier actividad relacionada con los recursos minerales, salvo la investigación científica, estará prohibida" (Secretaría del Tratado Antártico, 1991, p. 4), del cambiante panorama mundial pueden surgir giros inesperados en esta perspectiva: el Continente Blanco "en un futuro se vería enfrentado en un aumento de la presencia militar, mayores exploraciones, así como el aumento de estaciones de investigación producto de la importancia estratégica para las naciones" (Álvarez & Namen, 2019, p. 722).

Además de las oportunidades para el desarrollo científico colombiano en la Antártida, está el del ciberespacio como dominio y escenario virtual creado por el ser humano y que ya se encuentra involucrado en las distintas facetas de la vida cotidiana del hombre. Ambos *Global Commons* (Buck, 2013) representan desafíos de desarrollo, soluciones a los problemas de equilibrio frente al cambio climático y, sobre todo, respuestas de cara al futuro de la humanidad, trayendo consigo un desafío quizá mayor: mantener estas oportunidades dentro del marco de la seguridad global y seguridad internacional.

Teniendo esto en cuenta, se hace necesario precisar los retos y oportunidades del dominio ciberespacial de Colombia en la Antártida para 2042. A fin de establecer estos factores, se plantea el desarrollo del tema en tres instancias. En primer lugar, identificando las capacidades y las experiencias ciberespaciales de algunos países que participan en el Sistema del Tratado Antártico, para compararlas con la actual política de Gobierno en Colombia, y definir si el alcance de dicha política abarca el desarrollo de una infraestructura ciberespacial que cobije y proteja las actividades del Estado, especialmente las militares, en cualquier parte del mundo, y beneficie las actividades nacionales en la Antártida.

Lo anterior se evidencia a través del análisis de los casos de Estados Unidos, Rusia, China, Brasil, Uruguay y Argentina, como países que desarrollan actualmente actividades de exploración en la Antártida. Este análisis tiene como fin verificar el modelo y las medidas de protección asumidas. Los hallazgos son comparados con lo evidenciado en la revisión del Plan Nacional de Desarrollo Colombiano, la Política Nacional de Defensa, el CONPES y el Programa Antártico Colombiano. El propósito es dar cuenta de la existencia o inexistencia de capacidades cibernéticas en la Antártida, así como identificar el compromiso de estos países con la adquisición de capacidades ciberespaciales.

En segunda instancia, mediante fuentes documentales, analizar y dar cuenta de las capacidades ciberespaciales actuales y futuras de Colombia, sobre la base de lo propuesto en el Plan Nacional de Desarrollo (DNP, 2019) entre otras y en especial de la "Estrategia para el desarrollo Aéreo y Espacial de la FAC 2042" (FAC, 2020), la cual tiene objetivos trazados en la Antártida y permite reconocer en la FAC y en las mismas FF. MM. de Colombia una arquitectura cibernética que busca en el futuro la integración nacional con la Antártida.

Finalmente, se plantean los retos y las oportunidades que tiene Colombia para su participación permanente en la Antártida, a través del dominio ciberespacial, como resultado del desarrollo de los apartados anteriores, los cuales esperan ser sometidos a consideración posterior, tanto por la academia, como fuente de nuevas investigaciones, como por las FF. MM., Gobierno y entidades privadas, comprometidas en el futuro de Colombia desde su participación Antártica, como fuente de respuestas para el futuro del país. Se concluye con las consideraciones derivadas de la investigación.

Capacidades y experiencias de algunos países partícipes del sistema del Tratado Antártico en asuntos ciberespaciales

Con el fin de identificar las capacidades y las experiencias de diferentes países, directamente relacionadas con el uso del ciberespacio en la Antártida, se analizan los casos Estados Unidos, Rusia, China, Brasil, Uruguay y Argentina, miembros del Tratado Antártico. Seguidamente se verifica el modelo y las medidas de protección asumidas por cada uno de ellos. Los hallazgos son comparados con el Plan Nacional de Desarrollo Colombiano (DNP, 2019), la Política de Defensa y Seguridad Nacional (MDN, 2019), el CONPES y el Programa Antártico Colombiano (CCO, 2014). El objetivo del análisis documental comparativo es dar cuenta de la existencia o no de capacidades ciberespaciales colombianas en la Antártida, partiendo del compromiso de los países analizados, en la adquisición y fortalecimiento de capacidades ciberespaciales.

La Antártida representa una serie de oportunidades estratégicas para cada uno de los países que hacen parte del STA, puntos que fueron tratados en capítulos anteriores desde lo geopolítico, ambiental, aéreo y espacial. Para lo anterior, se parte del entendimiento de que el dominio ciberespacial es "la capacidad virtual de aplicar, controlar y aprovechar el ciberespacio para contribuir, mediante efectos en este y otros dominios. Su alcance es global y es aplicable en todo el rango de las operaciones" (FAC, 2020, p. 69).

Por lo anterior, aunque el dominio o las capacidades ciberespaciales de Colombia no han sido desarrolladas plenamente dentro del propio territorio colombiano y menos aún en la Antártida, es necesario comprender que el dominio ciberespacial es un escenario donde los demás dominios se encuentran inmersos y su desarrollo es cada día más complejo y sorprendente; por consiguiente, el mundo se enfrenta a una diversidad de amenazas de distinta naturaleza, ahora, en mutación ciber-. Estas amenazas afectan tanto el plano virtual y su componente físico, los cuales están anclados a "una geografía específica a través de cables de fibra óptica, satélites e instituciones" (Romero, 2019, p. 5), por lo tanto, analizar la arquitectura de estos sistemas ayuda a entender las relaciones de poder entre los Estados.

En respuesta a lo anterior, la Antártida ofrece "interferencias radiales en los ámbitos espaciales y ciberespaciales, que resultan ideales para la observación del espacio y el seguimiento de satélites". Esto abre paso fácil a la creación de

"redes de vigilancia y control remoto de sistemas ofensivos, o bien, cualquier otro de uso tecnológico" (Witker, 2015, p. 9). Lo importante es que Colombia amplíe la visión de la política pública establecida para la Antártida y genere las condiciones para proyectar una sombrilla ciberespacial a todas las actividades que viene desarrollando y las que vienen en los próximos años.

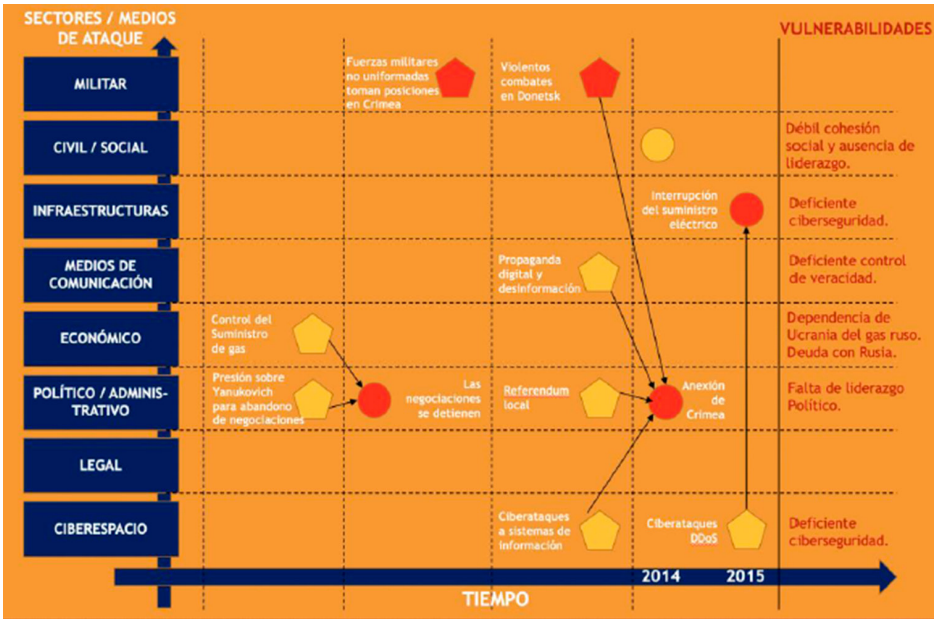
En este sentido y en un mundo cada día más dependiente de la dimensión digital, la defensa de este dominio requiere del desarrollo de unas capacidades tanto en el plano defensivo como en el ofensivo, aunque este último no debe considerarse para las actividades antárticas colombianas en concordancia con el TA y la Seguridad Internacional en el Polo Sur.

Lo anterior, por cuanto en el campo estatal pueden identificarse actividades de ciberespionaje exterior (político, militar, industrial, social), de cibersabotaje (infraestructuras militares y civiles, servicios esenciales, medios de comunicación), de ciberinterferencias en la vida colectiva de una sociedad o de vigilancia interna (Rizzi, 2022, p. 5).

Por lo tanto, el no controlar o ejercer acciones de seguridad en el campo ciberespacial representa una amenaza para los intereses de seguridad de los países. En palabras de Malekos (2022), "los países utilizan el poder cibernético para inclinar la balanza geopolítica" (p. 1). Adicionalmente, hay que dar por hecho que las organizaciones terroristas, el crimen organizado trasnacional y los países criminalizados cuentan con capacidades ciber- para realizar actos a ese nivel, lo que potencializa los riesgos y peligros de las amenazas tradicionales y las nuevas amenazas de la seguridad multidimensional (OEA, 2003).

Así las cosas y como se expresó en capítulos anteriores, el Tratado Antártico establece entre sus principios la protección del medioambiente y su uso desde una perspectiva pacífica y científica. Sin embargo, es necesario tener en cuenta que, en el panorama actual, las naciones están priorizando sus intereses particulares sobre los intereses globales, lo que puede evidenciarse en lo económico, la lucha por el predominio geopolítico, la expansión territorial en algunos casos y la búsqueda de recursos, por citar algunos casos. Un ejemplo de lo anterior es la confrontación entre Rusia y Ucrania que se inició desde hace varios años, con una serie de ataques híbridos como se presenta en la figura 1, donde puede identificarse el desarrollo de los medios de ataque frente al periodo en que transcurrieron estos, destacando en el campo ciber- el ataque a la interrupción del suministro eléctrico en 2015.

Figura 1. *Modelo de ataques híbridos: caso Ucrania*



Fuente: Galán (2018, p. 11).

Se evidencia, entonces, la necesidad de establecer como política de Estado, el uso del ciberespacio para la generación de la seguridad del Estado colombiano, frente a las amenazas multidimensionales a las que puede estar expuesto el país. Lo anterior va más allá de una política de Gobierno, cuyos periodos presidenciales no permiten la continuidad de la seguridad requerida; esto debe ampliarse a los escenarios mundiales a los que Colombia accede como es el caso del Tratado Antártico y las actividades nacionales en el Polo Sur.

A continuación, se presentan las cibercapacidades de los países que hacen parte del TA. Inicialmente, se estudian los países que se presentan como antagonistas o transformadores del actual orden mundial; posteriormente, se hace énfasis en los países de Suramérica que tienen capacidades y políticas en el ámbito ciberespacial.

Para analizar algunos países con cibercapacidades nacionales, se cita al *National Cyber Power Index 2020* del Belferd Center de la Harvard Kennedy School (Voo et al., 2020), donde, al respecto del interrogante de investigación por cuál es la nación cibernética más poderosa del mundo (p. iv), afirma que

los ciberactores del documento citado son respaldados por cada Estado, lo que podría representar una amenaza para la seguridad nacional, por cuanto cada uno de ellos busca dirigir sus esfuerzos para contrarrestar los ataques de otros, como fue el caso de Rusia frente a las elecciones en los Estados Unidos.

De igual forma, son presentados los siguientes diez países con la más alta intención y capacidades ciberespaciales, de acuerdo con siete objetivos nacionales identificados, dentro de los intereses propios de cada uno de ellos. La tabla 1 destaca esos diez países según los objetivos.

Tabla 1. *Diez países con mayores capacidades ciberespaciales según siete objetivos nacionales identificados*

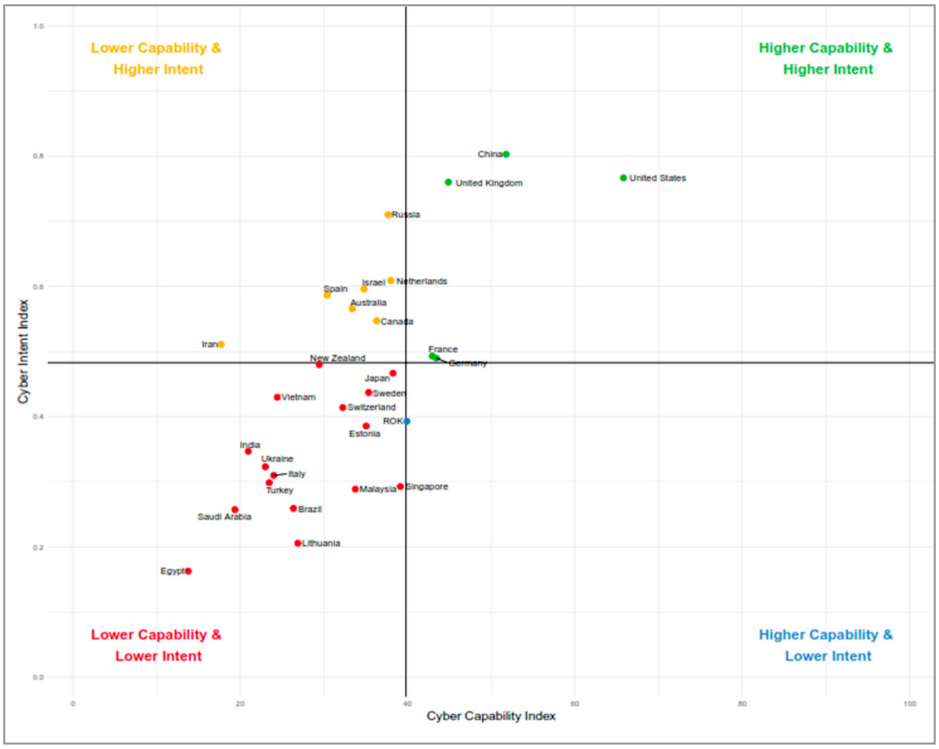
Los diez países más completos con el nivel más alto de intención y capacidades en los siete objetivos nacionales	Los siete objetivos nacionales identificados para alcanzar capacidades ciberespaciales
1. Estados Unidos 2. China 3. Reino Unido 4. Rusia 5. Países Bajos 6. Francia 7. Alemania 8. Canadá 9. Japón 10. Australia	1. Vigilancia y seguimiento de grupos domésticos. 2. Fortalecimiento y mejora de las defensas cibernéticas nacionales. 3. Control y manipulación del entorno de información. 4. Recolección de inteligencia extranjera para la Seguridad nacional. 5. Ganancia comercial o mejora del crecimiento de la industria nacional. 6. Destrucción o inutilización de las capacidades e infraestructura de un adversario. 7. Definición de normas cibernéticas internacionales y estándares técnicos.

Fuente: elaboración propia con base en Voo et al. (2020).

Adicionalmente, en la figura 2, se presenta la clasificación de los países con capacidades e intenciones cibernéticas, donde naciones del Tratado Antártico como Canadá, España, Países Bajos y Australia se mantienen dentro del grupo con algunas capacidades e intenciones ciberespaciales, mientras que Brasil, como único representante en el hemisferio americano, hace parte de los países con desarrollo ciberespacial, pero muy bajas capacidades en este sentido, lo que pone en contexto la brecha de cibercapacidades de los países en el mundo y los de la región más próxima a la Antártida. Colombia tampoco aparece dentro de los países con algún nivel de capacidades ciberespaciales, lo que representa un reto y oportunidad para que el país busque reducir las brechas respecto del

mundo y active un plan en el corto y mediano plazo para el desarrollo de sus actividades en el Continente Blanco.

Figura 2. *Clasificación de poder ciberespacial respecto de capacidad e intención*



Fuente: Tomado del Belferd Center de la Harvard Kennedy School (2020, p. 13).

Se evidencia un panorama de bajas capacidades ciberespaciales en la Suramérica próxima a la Antártida, mientras que las potencias mundiales compiten por los primeros lugares de supremacía ciberespacial, lo que presupone ventajas que pueden considerarse ilimitadas sobre el Continente Blanco, por cuanto no existe mayor información acerca de dónde y cómo se aplican estas capacidades, más allá de los siete objetivos nacionales delimitados por el Informe del Belferd Center, donde cada uno de ellos se enmarca en los intereses particulares de cada uno de los países en la Antártida, llevando a concluir una posible amenaza a futuro.

Cibercapacidades de Estados Unidos como referente mundial

En primer lugar, encontramos a EE. UU. en capacidades ciberespaciales, y, teniendo en cuenta las dificultades existentes para aplicar el marco disuasorio del ciberdominio, esta potencia ha desarrollado sus capacidades estratégicas en tres componentes: negación, resistencia y capacidades ofensivas (Reith, 2018, p. 57):

Disuasión por negación.

Se caracteriza por hacer inefectivas las armas ciberespaciales, de modo que un adversario se desanime incluso para tratar de efectuar un ataque.

Disuasión por resistencia.

Se caracteriza por esfuerzos cada vez más costosos, de modo que un adversario se desanime a atacar, aunque no se prevenga del ataque necesariamente. Los propietarios del exploit no pueden garantizar una posesión única, y con el tiempo dicha herramienta y dichas oportunidades a menudo se hacen obsoletas.

Disuasión por castigo (capacidades ofensivas).

Este tipo de disuasión se caracteriza por atacar directamente o amenazar con atacar directamente, al adversario, de modo que se le intimide de tal manera que no responda.

Además, y con el fin de desarrollar estas estrategias de ciberdefensa, EE. UU. cuenta con distintas agencias para la protección de sus intereses (tabla 2).

Tabla 2 . *Agencias de Estados Unidos para la protección de sus intereses*

Agencia	Objetivo
Cybersecurity & Infrastructure Security Agency (CISA)	Desarrollar, coordinar e implementar planes estratégicos, cuenta: División de Ciberseguridad Seguridad de Infraestructura Comunicaciones de Emergencia
Office of Management and Budget	Ciberseguridad federal en su conjunto
CISA Incident Reporting System	Provee los medios informáticos para reportar incidentes de ciberseguridad al CISA.
United States Cyber Command (USCC)	Cuya misión es dirigir, sincronizar y coordinar la planificación y las operaciones del ciberespacio, para defender y promover los intereses nacionales, en colaboración con socios nacionales e internacionales.

Fuente: elaboración propia con base en Jarufe (2022).

Con las agencias mencionadas, Estados Unidos desarrolla su estrategia de protección de sus activos estratégicos (activos y sistemas físico), los cuales, de no protegerse de manera efectiva, tendrían repercusiones tanto en su seguridad, economía, salud y otros sectores. Entre las áreas críticas por proteger de acuerdo con el CISA mencionado por Jarufe (2022), están:

- Sector químico.
- Instalaciones comerciales.
- Comunicaciones.
- Rubro manufacturero, las represas.
- Base industrial de la defensa.
- Servicios de emergencia, la energía, la alimentación, salud y agricultura.
- Oficinas de gobierno.
- Reactores nucleares.
- Sistema de transporte y agua.
- Sistemas de transporte (p.5).

Además de los siete objetivos nacionales generales, planteados por el Belferd Center de la Harvard Kennedy School, la estrategia de la ciberguerra de los Estados Unidos se fundamenta en el desarrollo de cinco pilares (Jiménez, 2015, p. 12):

- El ciberespacio con similar valor que los otros campos de la guerra.
- Mantenimiento de las ventajas tecnológicas
- Defensa proactiva en lugar de pasiva.
- La defensa colectiva.
- Protección de la Infraestructura crítica.

Aunque no existe una reclamación por parte de EE. UU. del territorio de la Antártida, su fuerte presencia en el Continente Blanco con sus tres bases permanentes, así como sus pequeñas bases de verano, campamentos y refugios, cuya producción científica requiere la protección de la distinta información desarrollada.

Cibercapacidades de Rusia y China, contrapeso en el entorno global

Para Rusia, la dependencia de los servicios de internet con EE. UU. es cada día más notoria; con el desarrollo de la Runet, se hace evidente la independencia con las compañías tecnológicas americanas (Jiménez, 2015, p. 19).

Así mismo, en conjunción con China, Rusia es cada día más convencido de la importancia del ciberespacio. De lo anterior, se han generado políticas bilaterales mediante la Organización de la Cooperación de Shanghái (OCS), publicadas en 2015, las cuales se denominaron "Reglas de Conducta en el Área de Seguridad de la Información" (Schreiber, 2019, p. 3), en estas, se detallan los lineamientos respecto de la seguridad de la información, es decir, la ciberseguridad. En particular, este documento "describe el objetivo de la propuesta, el cual es identificar los derechos de los Estados en el ciberespacio, promover y construir un comportamiento responsable en el mismo" (Schreiber, 2019, p. 3). En materia de ciberseguridad, tanto Rusia como China han desarrollado una serie de objetivos (tabla 3).

Tabla 3. *Objetivos rusos y chinos en materia de ciberseguridad*

Rusia	China
Soberanía digital —> Soberanía democrática.	Prevención del terrorismo, separatismo y extremismo.
Control sobre el flujo de información y libre flujo de la información.	Establecimiento y coordinación de cuerpos regionales antiterroristas.
En contra de la injerencia en los asuntos de otro Estado.	Salvaguardar la soberanía en el ciberespacio.
Proteger las libertades y derechos de los ciudadanos en el ciberespacio.	Gobernanza mundial justa y transparente.
Transparencia y desarrollo en el ámbito del ciberespacio.	Libre flujo de la información bajo los parámetros chinos.
Proteger la información e infraestructura crítica que pueda verse afectada en el ciberespacio.	En contra de la injerencia en los asuntos de otro Estado.

Fuente: elaboración propia con base en Schreiber (2019).

Así mismo, Rusia, en su política exterior "ya no tiene aspiraciones de integrarse en Occidente, todo lo contrario. [...] pretende establecerse como uno de esos nuevos polos de poder aislados cuyos intereses deben importar" (Jiménez, 2015, p. 22). De ahí se concluye que en el ámbito ciberespacial en la Antártida desarrollará sus capacidades individuales, primando sus intereses nacionales, además de establecer posiblemente un acuerdo de protección con su aliado China y aquellos países latinoamericanos afines con su línea ideológica.

Cibercapacidades de Brasil: hacia el desarrollo del ciberespacio regional

Brasil ocupa el puesto 18 a nivel mundial en el Índice Global de Ciberseguridad 2020 (ITU, 2022), y es el primer país en América Latina y el tercero en América en cibercapacidad. Como se citó en Pombo (2015), para el Ministerio de Defensa Brasileño, el poder cibernético se define como "la capacidad de utilizar el espacio cibernético para crear ventajas e influenciar eventos en todos los entornos operacionales y otros instrumentos de poder" (p. 5).

Para la defensa del campo cibernético, Brasil cuenta con las siguientes agencias: el Centro para la Gestión de Incidentes de Seguridad en las Redes de Computadoras (creado en 2006), el Centro para la Defensa Cibernética del Ejército (creado en 2010) y la oficina de Delitos Cibernéticos de la Policía Federal (creada en 2011).

Además de estas instancias, Brasil cuenta con los siguientes documentos que definen su estrategia de ciberseguridad: la "Estrategia Nacional de Defensa" (END), la "Política Cibernética de Defensa" (PCD) y la "Estrategia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal (2015-2018)".

Finalmente, Brasil no solamente enmarca su agenda con relación a la ciberseguridad mediante las instituciones y la normatividad vigente, sino que adelanta procesos de toma de decisiones y elabora normas sobre la gobernanza de la internet. Esto se evidencia con su participación activa en el Foro para la Gobernanza de internet (FGI) (Lobato, 2017, p. 10).

Respecto de la Antártida, Brasil cuenta con el Programa Antártico Brasileño (Proantar) que a su vez hace parte de la Política Antártica Brasileña (Polantar), esta última en revisión por parte del gobierno brasileño. Debido a esta articulación entre el Proantar, Polantar y los medios (Infraestructura) como bien lo expone Cardone (2021), "El programa científico antártico de Brasil evolucionó de una actividad subordinada a sus intereses de participar del régimen antártico a un programa altamente especializado, estructurado y articulado en función de metas científicas claramente definidas" (pp. 29-46).

Este reciente interés por parte de Brasil requiere a su vez de una integración con el aspecto ciberespacial, permitiendo además de garantizar la protección de la información, llevar a cabo las distintas labores de coordinación con el Brasil territorial y otros países del TA.

Cibercapacidades de Uruguay y su compromiso con el ciberespacio

Para 2018, Uruguay era el único país de Sudamérica con un alto compromiso en los cinco pilares del Índice Global de Ciberseguridad: legal, técnica, organizativa, desarrollo de capacidades y cooperación (ITU, 2018, p. 15). Como parte de su Política de Seguridad 2020-2025, el Ministerio de Defensa Nacional avanza en la creación del Comando Conjunto de Ciberdefensa, con el fin de generar las capacidades de disuasión conjunta y sectorial en el dominio ciberespacial (Ministerio de Defensa Nacional del Uruguay, 2020, p. 8).

Así mismo, en 2018 se creó el Centro Nacional de Respuesta a Incidentes de Seguridad Informática, cuyo objetivo es proteger los activos de información críticos del Estado, así como promover el conocimiento en seguridad de la información. Uruguay cuenta desde 2021 con una "Unidad de Cibercrimen [que es parte] de la Dirección de Investigaciones de la Policía Nacional, para enfocarse específicamente en *hackeos* que atenten contra la seguridad, confidencialidad e integridad de los sistemas informáticos" (Jarufe, 2022, p. 25). Para Uruguay la Antártida representa:

> Una visión estratégica del país, implica compromiso e inversión, para preservar la Antártida hoy, asegurando a las generaciones futuras el acceso a los derechos que nos puedan corresponder según el derecho internacional y a la proyección natural de nuestro territorio hacia el sur, objetivo permanente de nuestra exploración antártica. (Fontes, 2011, p. 137)

Al ser Uruguay, junto con Brasil, un referente regional en materia de la ciberdefensa, su modelo de gestión de protección de la información puede ser emulado por los demás países latinoamericanos y generar estrategias de protección en la Antártida desde el dominio ciberespacial con el fin de dar cumplimientos a sus líneas estratégicas en el Continente Blanco.

Cibercapacidades de Argentina

En Argentina se puede identificar una gran variedad en términos de normatividad, entidades y acciones para el desarrollo de las capacidades de ciberdefensa (tabla 4).

Tabla 4. *Capacidades de ciberdefensa de Argentina*

Capacidades	Objetivo
Comité de Seguridad de la Información	Decisión Administrativa N° 669/2004 artículo tercero, hace referencia al primer antecedente normativo para la ciberdefensa.
El ciberespacio para el sistema de defensa nacional	Grupo de trabajo entre el Ministerio de Defensa, Estado Mayor Conjunto y de las Fuerzas Armadas con el fin analizar desde el punto de vista técnico y normativo, las implicancias del ciberespacio para la Defensa.
Unidad de Coordinación de Ciberdefensa	Resolución del Ministerio de Defensa N° 385, del 22 de octubre de 2013 cuyo objetivo fue el desarrollo de capacidades y unidades especializadas para emergencias teleinformáticas.
Comando Conjunto de Ciberdefensa	Resolución del Ministerio de Defensa N° 343, del 14 de mayo de 2014 conducción de las operaciones de ciberdefensa.
Actualización de la Directiva de Política de Defensa Nacional	Decreto N° 2645/2014. Plantea la necesidad de desarrollar capacidades operacionales en la dimensión ciberespacial tendientes a adquirir competencias en los ambientes terrestres, naval y aéreo.
Dirección General de Ciberdefensa	Coordinación con organismos y autoridades de los distintos poderes del Estado, así como el control del Comando Conjunto de Ciberdefensa.
Política de Seguridad	Tiene la misión de asegurar los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos.

Fuente: elaboración propia con base en Lobato (2017).

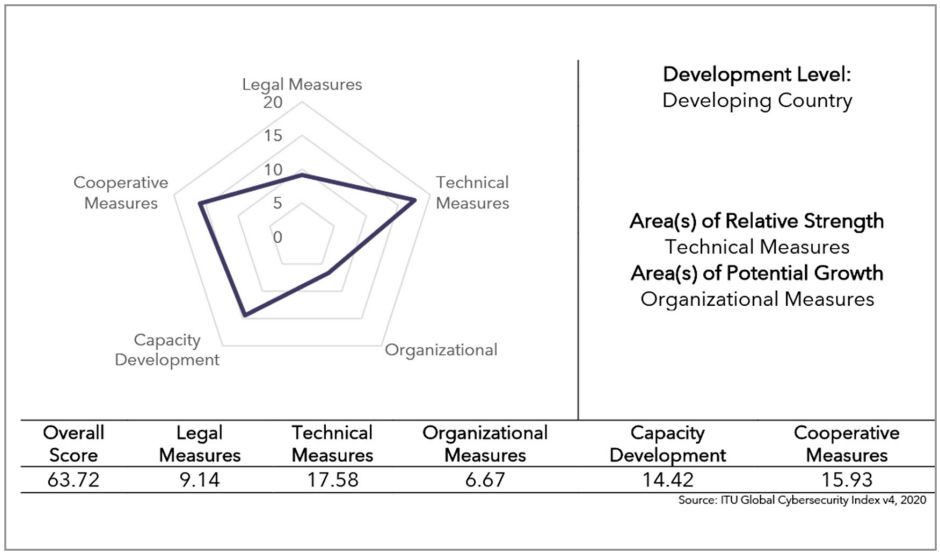
De acuerdo con lo expuesto, el modelo argentino se caracteriza por ser defensivo y hacer énfasis en el desarrollo de las capacidades en el dominio ciberespacial (Cornaglia & Vercelli, 2017, p. 14). Además, y aunque Argentina sigue desarrollando sus capacidades en el campo ciberespacial mediante las normatividades y entidades nombradas, también es cierto que tiene una fuerte presencia en la Antártida, gracias al desarrollo de sus trece estaciones, estaciones que requieren la protección de sus activos informáticos, lo que permite inferir que deberá ampliar sus capacidades en esta área para la protección de esta infraestructura.

Cibercapacidades de Colombia

Analizado el escenario mundial y con él algunos países parte del TA, corresponde revisar el caso colombiano. En contexto, el país ocupa el puesto 81 a nivel mundial en el Índice Global de Ciberseguridad 2020 que mide el compromiso con la ciberseguridad mediante las siguientes variables: la legalidad (normatividad), desarrollo de capacidades y cooperación. En la región hemisférica, se ubica en el puesto 9, y en Sudamérica, en el puesto 4, por debajo de países como Brasil (18), Uruguay (64), Chile (74) (ITU, 2022, p. 25).

A pesar de no poseer un lugar referente en el mundo y la región, Colombia ha construido algunas fortalezas y oportunidades de mejora en el campo de la ciberseguridad (figura 3).

Figura 3. *Compromiso de Colombia con la ciberseguridad*



Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
63.72	9.14	17.58	6.67	14.42	15.93

Source: ITU Global Cybersecurity Index v4, 2020

Fuente: Tomado del Índice Global de Ciberseguridad 2020 (ITU, 2022, p. 58).

Por otra parte, debido a la dependencia que actualmente se tiene de los sistemas digitales e informáticos, a partir de la primera década del siglo XXI el ciberespacio, y por ende la ciberseguridad, ha empezado a ser una prioridad para todos los países, en espacial aquellos con capacidad de desarrollo. No obstante, esta dependencia también genera una serie de vulnerabilidades (Orozco, 2021, p. 108).

Colombia no es ajena a esta realidad y a partir del CONPES 3701 de 2011 buscó "generar lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país" (CONPES, 2021, p. 2).

Además de lo anterior, se formaron grupos de trabajo y se incluyeron a las instituciones del Gobierno nacional (MDN, MinTIC, Ponal, etc.) y a las organizaciones del sector privado (representantes de los sectores de Energía y Comunicaciones, administradores de los dominios .co, universidades, etc.) (Sánchez et al., 2019, p. 177). Posteriormente, en 2014 se contó la asesoría de la Misión de Asistencia de la OEA para el desarrollo de marcos y políticas institucionales en el área cibernética. Para 2016, mediante el CONPES 3854, se creó la Política Nacional de Seguridad Digital con cinco objetivos específicos:

1. Crear el marco institucional en torno a la seguridad digital.
2. Crear las condiciones para que las múltiples partes interesadas gestionen el riesgo.
3. Fortalecer la seguridad de los individuos –del Estado en el entorno digital–.
4. Fortalecer la defensa y la soberanía nacional en el entorno digital (con un enfoque en gestión de riesgos).
5. Implementar las estrategias propuestas.

Aunque se han generado políticas y estrategias para enfrentar los distintos retos en materia de seguridad, según el Índice Global de Ciberseguridad (ITU, 2022), Colombia descendió del puesto 73 en 2019 al puesto 81 en 2020. Esto debe ser tomado como una alarma, y se deben identificar aquellos sectores o políticas que no ofrecieron los resultados esperados.

De acuerdo con lo expuesto en anteriores capítulos, aunque el interés por parte del Estado colombiano ha sido un tema recurrente en los últimos tiempos y se ve demostrado en el PAC, la llegada al Continente Blanco requiere de la protección de sus activos de información producto de las distintas actividades científicas.

En consecuencia, los documentos no evidencian un ciberdominio militar en la Antártida, de hecho, se relaciona más con el desarrollo tecnológico y científico que hasta ahora se está consolidando en esa zona. Esto quiere decir que no existe una infraestructura crítica cibernética suficientemente desarrollada para

hablar de ejercer un dominio militar; son pocas las naciones que ejercen una presencia permanente, recordando que el TA evita cualquier disputa sobre ese territorio, solo actividades científicas. Metodológicamente, lo que se podría proponer es que, con la tecnología a la mano de la ciencia, se busque proyectar el poder nacional en el Polo Sur; esto implica el desarrollo del poder naval, terrestre, aéreo apoyado en la tecnología. "Destacando que para ejercer un dominio en ese territorio debe establecerse primero una presencia permanente", esto implica considerar adecuar tecnología y capacidades para el ejercicio del poder en ese territorio de manera blanda. La tabla 5 muestra el comparativo de las capacidades de los países presentados.

Tabla 5. *Comparativo cibercapacidades de algunos países integrantes del TA*

País	Puesto en el Índice Global de Ciberseguridad	Desarrollo de Políticas de ciber seguridad	Operaciones Militares Ciber-	Combate al cibercrimen
EE. UU.	1	100 %	100 %	100 %
Rusia	5	86 %	100 %	78 %
Brasil	18	57 %	44 %	100 %
China	33	14 %	50 %	44 %
Uruguay	64	20 %	50 %	33 %
Colombia	81	29 %	67 %	100 %
Argentina	91	86 %	67 %	67 %

Fuente: elaboración propia con base en ITU (2022).

Proyección de cibercapacidades de la Fuerza Aérea aplicables en la Antártida

La FAC, como institución del Estado colombiano e institución estratégica para la integración del país con la Antártida —como se presentó en el capítulo anterior— ha venido desarrollando sus propias capacidades ciberespaciales en beneficio, no solo de la misma Fuerza, sino del Estado en pro de los objetivos nacionales, intereses nacionales y estrategia de Seguridad y Defensa nacionales, sabiendo que, como se mencionó, aún falta mucho por planear y fortalecer de la ciberseguridad del Estado colombiano en la Antártida. Por lo tanto, el presente apartado

tiene por objeto analizar los documentos fuente que evidencian las capacidades y ver capacidades especiales futuras de la Fuerza Aérea aplicables en la Antártida.

Antecedentes del desarrollo ciberespacial en la FAC

Desde 2018, la FAC desarrolló un proceso de transformación de su estructura organizacional de cara a enfrentar los distintos retos en materia de seguridad. Por esto, con la Disposición N.o 061 del 22 de diciembre de 2018, se reestructura la organización de la FAC y con ella la Dirección Cibernética Aérea y Espacial (DICAE), cuya misión es la realización de operaciones de ciberseguridad y ciberdefensa a través del desarrollo de sus capacidades con el fin de proteger la infraestructura aeronáutica critica de la Fuerza (Fuerza Aérea Colombiana [FAC], TOE código N.o 4-03-08-20).

Así mismo, para el cumplimiento de su misión, la DICAE cuenta con dos subdirecciones: la Subdirección de Ciberseguridad (SUCSA) y la Subdirección de Ciberdefensa (SUCDA). Esta última es "la encargada de proteger la infraestructura crítica militar aeronáutica de la Fuerza. Inclusive la del país y también tiene la responsabilidad de dar respuesta ante un ataque cibernético a nuestra infraestructura crítica" (FAC, TOE código N.o 4-03-08-20).

De acuerdo con la Tabla de Organización de Equipo de la Fuerza (TOE) código N.o 4-03-08-20), la SUCDA emite las políticas para evitar o para que se trabaje el proceso de conocer las herramientas cibernéticas que tiene el enemigo para hacer daño con la ciberinteligencia; también cuenta con la cibercontrainteligencia, cuyo objetivo es adoptar medidas para prevenir y neutralizar esos ataques (Subjefatura Estado Mayor de Estrategia y Planeación, 2020, p. 4). Organizacionalmente, la DICAE depende del Comando de Operaciones Aéreas (COAES), Jefatura de Inteligencia Aérea (JEINA) (figura 4).

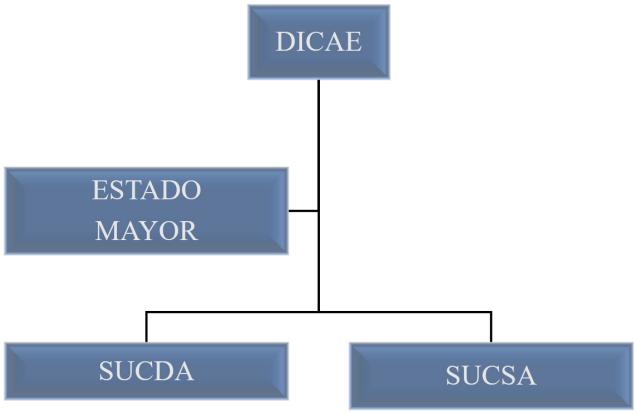
Entre las funciones de la DICAE, pueden destacarse las siguientes (Subjefatura Estado Mayor de Estrategia y Planeación, 2020):

- Emitir y establecer políticas y lineamientos de desarrollo de operaciones de ciberdefensa en la FAC .
- Definir y establecer políticas y lineamientos de desarrollo de operaciones de ciberseguridad en la FAC, con el propósito de proteger y asegurar el componente tecnológico de la infraestructura crítica.
- Fijar y emitir políticas y lineamientos de las actividades de investigación, desarrollo e innovación en la Fuerza Aérea que contribuyan a generar y

fortalecer las capacidades cibernéticas para el desarrollo de operaciones de ciberdefensa y ciberseguridad.

- Definir y establecer políticas y lineamientos para el análisis cibernético y prospectivo en la Fuerza Aérea.

Figura 4. *Estructura organizacional DICAE*



Fuente: elaboración propia con base en TOE código N.o 4-03-08-20.

Actuales capacidades ciberespaciales de la Fuerza Aérea

Garantizar el control del ciberespacio por parte de una organización representa un gran reto, debido a las características inherentes a su dominio. A continuación, se describen los conceptos relacionados con los intereses del dominio ciber-, desarrollados en el marco de análisis del objetivo N.° 2, a manera de propuesta:

Alcance.

La ausencia de fronteras permite desarrollar ciberoperaciones desde cualquier parte del mundo.

Asimetría.

El acceso al ciberespacio es sencillo y económico, lo que puede incrementar la capacidad del enemigo para acceder a medios tecnológicos para atacar. Se podría hablar de una "democratización" de estos: una persona con un computador y una conexión a internet puede realizar un ataque con resultados estratégicos sin el empleo de armento convencional y a un bajo costo.

Anonimato.
La facilidad de ocultar al individuo y organizaciones en el ambiente virtual.

Tempo.
Debido a las técnicas y la complejidad de los medios empleados, las acciones en el ciberespacio requieren de mayor preparación en comparación con el uso de medios cinéticos.

Versatilidad.
Empleo de medios ya anteriormente usados. Uso del recurso de la misma organización. (Gutiérrez, 2021, p.5).

Además, con el fin de enfrentar estas características del campo ciberespacial, la FAC, a través del Manual de Doctrina Básica Aérea, Espacial y Ciberespacial (FAC, 2020) ha establecido para su desarrollo, las siguientes capacidades distintivas:

- Garantizar, mediante el empleo de las capacidades ciber-, la superioridad ciberespacial con el fin de permitir la conducción de operaciones aéreas y ciberespaciales.
- Desarrollar operaciones aéreas y ciberespaciales espaciales a fin de garantizar la superioridad ciberespacial en el Rango de las Operaciones Militares (ROM), por medio de la integración de recursos, protección y tecnología con sistemas de información que por su diseño facilitan la multiplicación y soporte de las capacidades de otras (FAC, 2020).
- Multiplicar el poder aéreo y espacial usando el ciberespacio: empleo de cursos de acción no convencionales con tecnologías disruptivas y análisis de información a fin de maximizar los efectos del empleo de estos (FAC, 2020).

En el aspecto doctrinario, la Fuerza Aérea publica en 2015 el Manual de Ciberdefensa y Ciberseguridad O-MACIB, que establece las distintas responsabilidades de la Fuerza en el Ciberespacio. Así mismo, las FF. MM., para 2016, desarrollan el Manual de Ciberdefensa Conjunta como el documento de mayor jerarquía y que tiene como objetivo unificar los diferentes conceptos en el desarrollo de operaciones conjuntas en el dominio ciberespacial, permitiendo la integración de las capacidades cibernéticas de cada una de las FF. MM., todo bajo la supervisión del Comando Cibernético (Comando General de las Fuerzas Militares, 2016).

Capacidades ciberespaciales futuras de la Fuerza Aérea aplicables en la Antártida

Como se enunció en el capítulo anterior, la FAC ha desarrollado cuatro campañas en la Antártida durante los periodos 2015, 2017, 2019 y 2020. De esta forma, apoyó con sus capacidades aéreas los objetivos del Programa Antártico Colombiano (PAC), "el cual se ha convertido en la hoja de ruta que hará posible la materialización de los intereses nacionales en ese territorio" (CCO, 2014, p. 7). Sin embargo, en el orden ciberespacial, las citadas expediciones tuvieron operaciones de ciberseguridad a las actividades nacionales en el Polo Sur.

Paralelo a este tipo de actividades, desde 2019, la FAC realiza un ejercicio de capacidades denominado "Estrategia para el desarrollo aéreo y espacial de la FAC 2042 (EDAES)", que desarrolla la visión y las capacidades en un horizonte 2022, 2030 y 2042, con el fin de enfrentar los distintos desafíos en materia de seguridad de forma eficiente y en multitud de escenarios. Asimismo, está alineado con la Política de Defensa y Seguridad para la Legalidad, el Emprendimiento y la Equidad y el Plan Estratégico Institucional, cuyos dos objetivos guían el desarrollo de las capacidades ciberespaciales de "sostener, preservar y proteger el Poder Aéreo, Espacial y Ciberespacial, [así como de] fortalecer las Capacidades del poder Aéreo, Espacial y Ciberespacial" (FAC, 2020, p. 63) y direccionan el devenir ciberespacial colombiano.

Para lo anterior, la FAC en el EDAES cuenta con el Plan de Desarrollo, el cual se "soporta en un análisis prospectivo que permite definir las principales características que debe tener la institución en los horizontes de tiempo anteriormente nombrados" (2020, p. 52). El plan ha sido desarrollado de acuerdo con una Proyección Morfológica, en la cual, para 2042, se destaca en el componente de infraestructura, la "Contribución de soporte para la operación permanente de la Estación Científica Antártica Colombiana" (p. 53).

Así mismo, y con el fin de dar protección a la infraestructura por desarrollar en la Antártida, la Fuerza Aérea ha planteado desarrollar sus capacidades, primero de ciberdefensa, la cual considera que debe estar operando permanentemente, además de tener la posibilidad de buscar y mantener los niveles apropiados de protección "de las infraestructuras críticas frente a las amenazas en el ciberespacio" (p. 70), y segundo, de ciberseguridad, la cual se plantea como respuesta a las "amenazas y el ataque en el ciberespacio" (p. 70).

Además, si algo caracteriza al dominio ciberespacial es la alta capacitación que debe tener el talento humano, para lo cual DICAE ha venido trabajando en el

desarrollo del plan de carrera de este personal, llevando a capacitar al personal de oficiales en Estonia con el fin de contar con las habilidades y capacidades en este campo. Así mismo, desde 2003, la FAC estableció el Programa de Ingeniera Informática en la Escuela Militar de Aviación (EMAVI), con el objetivo de preparar a los futuros oficiales para desempeñarse en las áreas de telecomunicaciones, sistemas de información geográfica, desarrollo de *software* y ciberseguridad.

Así como se expresó, las capacidades en el área profesional, la FAC prepara al personal de suboficiales en el desarrollo del campo técnico y practico, con el fin de capacitarse en competencias específicas. En este orden de ideas, la Escuela de Suboficiales (ESUFA) ofrece entre su variedad de programas tecnológicos, la Tecnología en Inteligencia Aérea, donde se destaca la siguiente área de conocimiento aplicable en el dominio ciberespacial: conocer y dominar las herramientas de seguridad de la información (manejo, almacenamiento, custodia, encriptación).

Por medio de este talento humano profesional y técnico, la Fuerza Aérea busca enfrentar las distintas amenazas en el ciberespacio. Además de lo anterior, dentro de los distintos proyectos por tener en cuenta para 2042 en el dominio ciberespacial, existen algunos que podrán ser empleados en la protección de la infraestructura en la Antártida con el fin de investigar y responder a las distintas amenazas o ataques de naturaleza cibernéticas que se puedan presentar en el Continente Blanco.

Retos y oportunidades de Colombia en la participación del dominio ciberespacial en la Antártida

Desde tiempos antiguos, la naturaleza social del ser humano ha condicionado su desarrollo dentro de estructuras colectivas; este relacionamiento lo supedita a buscar posiciones de protección y resguardo frente a los riesgos y peligros que puedan afectar su bienestar, familias o bienes, trayendo consigo desafíos en términos de seguridad y defensa que en la contemporaneidad se han denominado *amenazas* (OEA, 2003). Con el desarrollo de la sociedad, también se dio la evolución, alcance y diversidad de dichas amenazas; el ser humano vive en medio de la incertidumbre respecto del peligro que le rodea, más aún si considera que no tiene las garantías estatales o gubernamentales en materia de seguridad.

Aunque esta situación varía de una sociedad a otra, como lo expresa Cancelado (2010) "la percepción de amenaza cambia y en nuestro siglo, influenciado por un proceso de globalización sin precedentes, los efectos de la interconexión humana también interconectan las percepciones de amenaza y seguridad" (p. 2), llevando a que se busque protección desde lo supranacional.

La globalización ha generado que, en su multiplicidad, las amenazas hayan mutado y sean ahora transnacionales, ocultas y desarrolladas en una variedad de campos de batalla. De hecho, desde 2005 se vislumbraban distintos fenómenos que actualmente tienen total vigencia, más aún, si se desarrollan en ambientes como el ciberespacio. En este sentido, según el National Intelligence Council de los EE. UU., se debe al creciente proceso de globalización del presente siglo XXI que resulta irreversible y, por lo tanto, los actores no estatales se hacen cada vez más visibles y juegan un papel mucho más preponderante (Avilés, 2005).

Esta situación se acentúa en el ciberespacio debido a las características especiales que posee este dominio virtual creado por el hombre, entre las que se destacan "la extensión, el anonimato, la inmediatez y su fácil acceso [que por] su carácter artificial y su rápida evolución, generan continuas vulnerabilidades y oportunidades" (Gobierno de España, 2018, p. 71), además, debido a su transversalidad, puede generar zonas grises en combinación con los dominios marítimos, aéreo y espacial.

Por lo anterior, estrategias como la establecida por el Gobierno colombiano de acceder a la Antártida en el marco del Tratado Antártico, la investigación científica nacional, la búsqueda de respuestas a soluciones de medioambiente y la participación en la seguridad internacional, requieren un alto grado de protección respecto de las amenazas que pueden provenir del terrorismo o la criminalidad desde el ciberespacio. Teniendo en cuenta que el análisis realizado en la presente investigación devela que la Agenda Antártica Colombiana no tiene establecida una propuesta de protección en materia de ciberdefensa y ciberseguridad, se hace necesario establecer una estrategia ciberespacial que garantice las condiciones de seguridad frente a estas, no tan nuevas, amenazas.

Para tales efectos, se plantean los retos y oportunidades que esta investigación ha formulado, esperando signifiquen un aporte a la generación de nuevo conocimiento y sean materia de análisis en el marco de la Agenda Antártica Colombiana.

Retos y oportunidades para un escenario ciberespacial colombiano en la Antártida

En el desarrollo del presente capítulo se presentaron las cibercapacidades de algunos países latinoamericanos pertenecientes al TA, así como de Colombia y, en especial, de la Fuerza Aérea; teniendo en cuenta que, si bien existe una política de Estado en ciberdefensa y seguridad y una política pública respecto de la Antártida, es necesaria la integración de los elementos en ambas políticas para generar un marco de ciberseguridad colombiana en la Antártida.

Debido al carácter furtivo del ciberespacio, donde un ataque puede provenir de cualquier parte del mundo, en materia de costo-beneficio la ejecución de acciones a una economía mucho menor que los costos que se pagan por mantener aviones, buques, tanques y soldados con armamento militar convencional; de alguna manera, esto puede suprimir y negar cualquier superioridad militar, llegando a afectar la infraestructura de un país, sus equipos y, en general, la seguridad de los seres humanos víctimas de ciberataques. Por lo tanto, se hace necesario desarrollar las acciones para mitigar el riesgo en el ciberespacio, más aún, cuando Colombia se encuentra desarrollando actividades en la Antártida.

En este orden de ideas, aunque Colombia trabaja por mantener una presencia activa en la Antártida, mantiene firme su propósito de cumplir uno de sus los objetivos específicos, "desarrollar e implementar la capacidad logística del país en infraestructura y equipamientos adecuados, para facilitar la presencia activa y permanente del país en la Antártica", Estación Científica de Verano "Almirante Padilla" (CCO, 2014, p. 17) y, por lo tanto, debe garantizarse la protección de la información y los resultados de los distintos trabajos científicos, activos informativos, equipos de investigación e infraestructura, empleados en el propio desarrollo antártico colombiano.

Por lo tanto, y desde el enfoque de López (2012), la pregunta por responder en materia de ciberdefensa es la de quién debe proporcionar la seguridad "en las redes y sistemas de información" de los activos desarrollados por Colombia en materia de investigación, asuntos geopolíticos colombianos y de participación nacional de la seguridad internacional (p. 154).

Aunque existe poca información y registro en materia de ataques cibernéticos a los países que participan en la investigación en el continente antártico, lo cierto es que en 2004, "un grupo de *hackers* rumanos estuvieron a punto de poner en peligro las vidas de 58 investigadores que trabajaban en una misión científica en la Antártida" (Echevarría, 2009, p. 3), denotando que las ciberamenazas

contra la seguridad de los países, incluso aquellos con capacidades más robustas, es una realidad de la que Colombia no está exenta.

La investigación plantea al respecto algunos retos y oportunidades (tabla 5) que, en materia ciberespacial, puede adoptar el Estado colombiano en pro de la creación de una infraestructura de ciberseguridad y ciberdefensa, para proteger no solamente las operaciones aéreas y navales hacia el Continente Blanco, sino también la información, la investigación científica y el factor humano.

Tabla 6. *Retos y oportunidades del ciberespacio en la Antártida*

	Retos	Oportunidades
1	Contrarrestar las acciones de desinformación y decepción.	Establecer o adherirse a un marco común de ciberseguridad ajustando el TA.
2	Enfrentar los ataques cibernéticos.	Integrar a Colombia a las capacidades ciber- de los países del TA.
3	Reducir las tensiones de un conflicto armado internacional.	Establecer o adherirse a un marco común de ciberseguridad ajustando el TA.
4	Enfrentar el ciberterrorismo.	Integrar a Colombia a las capacidades ciber- de los países del TA.
5	Afrontar el ciberespionaje.	Crear la protección requerida para las futuras capacidades ciber- en la Antártida.
6	Contrarrestar las acciones de erosión de la cohesión social.	Establecer o adherirse a un marco común de ciberseguridad ajustando el TA.
7	Contrarrestar la afectación de avances tecnológicos adversos.	Crear la protección requerida para las futuras capacidades ciber- en la Antártida.
8	Combatir el crimen organizado.	Integrarse a las capacidades ciber- de los países del TA para enfrentar la amenaza.
9	Integrar el dominio ciber- en la Antártida.	Buscar puntos de acuerdo entre las políticas relacionadas con la Antártida y lo relacionado con el ciberespacio en Colombia, así como la integración académica y estatal relacionada con esta materia.

Fuente: elaboración propia.

Marco Común de Ciberseguridad ajustando el TA

Existe una variedad de amenazas como las acciones de desinformación y decepción, entendidas como "la sobreabundancia de fuentes de información, circunstancias que disminuyen la capacidad de análisis y favorecen la proliferación de fenómenos de manipulación informativa: difusión de bulos, desinformación, decepción, etc." (Gutiérrez, 2021, p.4), que añaden desconcierto e imaginarios en la población, exacerbando la desconfianza y sensación de peligro; de igual

manera, algunas otras se encuentran asociadas a las acciones de erosión de la cohesión social, que se desprenden de las falencias de integración entre los miembros de una sociedad y que redundan en desigualdad, la pérdida de capital social, aumento de la pobreza y una serie de componentes que amenazan con el bienestar individual y, en consonancia, la productividad colectiva. De acuerdo con el Informe de Riesgos Globales 2022, del Foro Económico Mundial, la erosión en la cohesión está en el cuarto puesto. "Para 2030, se proyecta que 51 millones de personas más vivirán en la pobreza extrema en comparación con la tendencia anterior a la pandemia una recuperación económica desigual corre el riesgo de aumentar la polarización y el resentimiento (World Economic Forum, 2022, p. 16).

Cuando se firmó el TA el 1 de diciembre de 1959, nadie tenía entre sus perspectivas el desarrollo del dominio ciberespacial y mucho menos, las distintas variedades de amenazas que podrían afectar este dominio. Hoy, las amenazas representan un reto para contrarrestar, ya que, por un lado, pueden generar desinformación de los trabajos científicos desarrollados, y, por otro lado, acciones de erosión de la cohesión social pueden generar espacios de controversia donde los intereses de unos particulares interfieran en el concepto inicial del TA.

Una oportunidad para enfrentar estos retos es con el desarrollo en el TA de un marco común de ciberseguridad ajustado a los intereses tanto de los países con características de miembros consultivos, como de los no consultivos.

Aunque la Antártida es un territorio de paz y, por ende, las actividades militares están prohibidas, también es importante tener en cuenta las coyunturas globales y, en especial, desde el dominio ciber- donde la explotación de recursos cibernéticos ha potencializado las tensiones en el mundo, afectando el poder militar de una manera no tradicional ya que, además, le impacta económicamente (Delgadillo, 2018, p.5), sumado a lo anterior, con la variedad de recursos naturales en la Antártida se hace necesario incluir en el MCC unos lineamientos para la protección de los recursos cibernéticos de los Estados del TA.

Integración de capacidades ciber- de los países del TA

Otro de los retos para desarrollar es contrarrestar las distintas amenazas de ataque cibernético, crimen organizado, ciberterrorismo. Los ataques cibernéticos son una amenaza inquietante ya que afectan directamente el capital informático y pueden impactar mucho más allá del factor económico o físico. Para Jiménez (2015), "Tienen como objetivo un ordenador o un sistema y la información que contenga, y aunque pueda conllevar en algún momento a daño físico, siempre

va a estar centrado en dañar lo informático" (p. 10). Es decir, que mediante un ciberataque se podrían afectar los equipos e instalaciones que controlan las distintas misiones que se desarrollan en el Continente Blanco, cuyas consecuencias dependerán de la intensidad de aquel, pudiendo variar desde una pérdida insignificante de información o la afectación de infraestructura vital. Teniendo en cuenta la amplia variedad de recursos que tiene la Antártida y en la medida que los medios tecnológicos se sigan desarrollando para facilitar su explotación, el crimen organizado puede encontrar en el ciberespacio la alternativa para hacerse a lo mismo. Finalmente, puede encontrarse una singular variedad de categorías en términos de ciberterrorismo ampliamente abordado por Delgadillo (2018):

Propaganda.
Comprende el uso de estrategias de audio o video que buscan difundir ideologías que se basan en la autojustificación para persuadir, reclutar, radicalizar o incitar al terrorismo (p. 8).

Financiación.
"La recaudación puede ser de cuatro tipos generales, la recaudación directa, comercio electrónico, empleos de pago en línea —PayPal o Skype— y contribuciones a organizaciones benéficas" (p .8).

Adiestramiento.
"Existen también campamentos virtuales terroristas que emplean las diversas plataformas para difundir archivos multimedia de cómo fabricar armas o explosivos, asesorar la planeación y ejecución de ataques terroristas, así como proporcionar herramientas para realizar acciones de inteligencia" (p. 8).

La planificación.
"Obtención de información de dominio público, enlaces de comunicaciones y cualquier contenido que permita fortalecer las capacidades para efectuar un acto terrorista" (p. 9).

La ejecución.
"Empleo del ciberespacio y del internet permiten efectuar coordinaciones previas a la ejecución de un acto terrorista, tener contacto con sus personas objetivos o incluso pueden transmitir en tiempo real sus acciones de violencia extrema" (p. 9).

Debido a la capacidad del ciberespacio de ser accesible para la gran mayoría de la población, es factible el empleo de este dominio para la preparación desde cualquier lugar del mundo de un ataque terrorista a la Antártida, afectado la seguridad de las personas y de los descubrimientos científicos. Adicionalmente, el anonimato que presenta y la dificultad de judicialización de los actores antagonistas permiten a estos actuar sin ética ni moral, pudiendo desarrollar actividades terroristas de gran impacto en este continente.

En la medida que la tecnología avance será más fácil para los distintos antagonistas materializar toda esta serie de amenazas anteriormente expuestas, por lo que se requiere un accionar conjunto mediante la integración de las cibercacapidades de los Estados firmantes del TA.

Protección de las futuras capacidades ciber- en la Antártida

Como se ha mencionado, Colombia todavía no desarrolla una infraestructura permanente en la Antártida, Sin embargo, es necesario adelantarse a los acontecimientos y desarrollar el componente ciberespacial en la Antártida con el fin de garantizar la protección de los activos físicos y digitales en este ambiente. De acuerdo con Stel (2014), "El ciberespacio impone grandes desafíos mentales. El modelo de pensamiento tradicional, lineal y convencional, colisiona con el pensamiento cibernético, el cual es asimétrico y atemporal" (p. 39), esto implica no solo el desarrollo de políticas o lineamientos en las instancias gubernamentales, sino que requiere de procesos de adiestramiento, actualización y apertura de pensamiento frente a las nuevas amenazas. Dentro de las distintas ciberamenazas que pueden enfrentar las instalaciones colombianas, puede evidenciarse el ciberespionaje, que basa sus acciones en la obtención de información secreta de personas, instituciones o Gobiernos mediante el uso de las tecnologías de la información con fines maliciosos que pueden tener connotaciones económicas, estratégicas e incluso bélicas lo cual se presenta como un instrumento estratégico contra los actores internacionales.

Hay que tener en cuenta que los países también buscan extender su control por medio de la infiltración de los sistemas informáticos de otros Gobiernos, con el fin de extender sus influencias tanto a nivel regional como externo, en este caso la Antártida, por lo que Colombia debería estar preparado para enfrentar dichas amenazas.

Otro asunto es la velocidad del desarrollo de los avances tecnológicos, ya que según Realpe y Cano (2020), "genera un espacio propicio para la incubación

de amenazas cibernéticas, que pueden poner en riesgo la prosperidad económica y social de un país, así como su Seguridad y Defensa nacionales" (p. 2), denotando un gran reto para Colombia en términos de competitividad en temas cibernéticos que le sitúen en una posición ventajosa frente a dichas amenazas.

Sin embargo, no necesariamente esta ventaja se remite de manera exclusiva, ni mucho menos, extrema de procesos de permanente actualización; en este sentido, cabe anotar que, en las inspecciones en el marco de las Reuniones Consultivas del Tratado Antártico efectuadas por Noruega en 2018, se consideró:

> Que existía una tendencia sostenida a adoptar sistemas tecnológicos más complejos que permitirán la operación remota en mayor medida que los sistemas anteriores. Se indicó que esto genera oportunidades nuevas e interesantes en relación con la eficiencia operativa, las operaciones autónomas y la recolección remota de datos, entre otros aspectos. Pero que también podría generar algunos riesgos, ya que las estaciones serían más vulnerables y dependerían de personal especializado, además de estar expuestas a riesgos cibernéticos. (Lazen 2019, p. 4)

En vista de lo anterior, y sabiendo que la tendencia de amenazas en el campo ciber- no pretende disminuir debido al aumento del uso de *software y hardware* en las actividades diarias, más en el campo científico y, en especial, en la Antártida donde el uso de sistemas para la difusión de la información se dificulta por las adversidades del terreno, es importante tener en cuenta lo aportado por Becerra (2019), cuando consideró que "la gestión del riesgo y la gobernanza representan dos de las herramientas más importantes para el fortalecimiento de las capacidades de los Estados en materia de ciberseguridad y ciberdefensa" (p. 111).

Conclusiones

En el TA se "designa la Antártida como reserva natural, consagrada a la paz y a la ciencia" (Secretaría del Tratado Antártico, 1991, p. 1) Aunque desde su firma, los miembros consultivos y aquellos no consultivos han desarrollado sus actividades científicas bajo un marco de entendimiento y los incidentes en materia ciber- son mínimo o no están documentados, lo cierto es que se vive en un mundo cambiante donde los intereses de supervivencia de los países prima sobre los distintos marcos comunes. El desarrollo del proceso de investigación sugiere considerar las siguientes conclusiones:

Entre los países estudiados pertenecientes al TA existe una variedad de niveles de desarrollo de las capacidades ciber-, siendo los EE. UU. el referente, pues ocupa el primer puesto según el Índice Global de Ciberseguridad (International Telecommunication Union [ITU], 2022), seguido de China y Rusia. Por otra parte, en Latinoamérica se toma una muestra de los países consultivos del TA Argentina, Brasil, Uruguay y por último Colombia, los cuales emplean sus capacidades ciber- para la defensa de sus intereses nacionales en mayor o menor grado de desarrollo, sin embargo, no fue posible identificar lo referente a la aplicación de dichas capacidades en el Continente Blanco.

Con relación a la FAC, de un tiempo para atrás ha venido haciendo énfasis en el aumento de las capacidades para la defensa del ciberespacio, lo cual se ve identificado en varios niveles: desde el nivel doctrinal con la incorporación de dominio ciber- en la función de dominar el aire, el espacio y el ciberespacio, a nivel organizacional con la creación de la DICAE, encargada de la ciberseguridad y ciberdefensa; a nivel de personal con el desarrollo del plan de carrera para los oficiales y suboficiales de la Fuerza, y la proyección a 2042 donde no solamente se integra las capacidades ciber-, sino el compromiso con el desarrollo de los proyectos de investigación científica en la Antártida.

En cuanto a retos y oportunidades en la Antártida, desde el punto de vista del dominio ciber-, se encontraron distintas ciberamenazas que se asumen como retos y para las que puede generarse una serie de cursos de acción a fin de contrarrestar o minimizar los riesgos en caso de que se materialicen:

- Buscar puntos de acuerdo entre las políticas relacionadas con la Antártida y lo relacionado al ciberespacio en Colombia, así como la integración académica y estatal.
- El dominio ciber- se caracteriza por su transversalidad en los otros dominios, por lo que es importante para el Estado colombiano poseer y desarrollar las capacidades ciber- en sus distintas áreas de interés, con el fin de garantizar el control y permanencia en los otros dominios y en este caso particular en la Antártida.
- Al ser el dominio ciber- de naturaleza humana, está continuamente amenazado por una gran variedad de agentes desestabilizadores, los cuales no solamente pueden atacar un país, sino también una región, en este caso la Antártida; es relevante desarrollar un marco común de cooperación en materia ciber- entre los países del TA para enfrentar las amenazas comunes, así como unos principios con el fin de ser integrados en el TA.

- Los distintos desarrollos tecnológicos no solamente presentan una oportunidad de ampliación de capacidades, sino que también pueden ser empleados como actores generadores de riesgos para los países del TA, en especial, para Colombia. Por lo anterior, se plantean algunas alternativas para enfrentar dichos riesgos:
    - Generar una independencia ciber- para la no dependencia de terceros con el fin de garantizar la protección del personal y los activos físicos y de información.
    - Desarrollo de proyecto I+D+i con el fin de integrar el dominio ciber- con la Antártida, identificando puntos comunes de desarrollo.
    - El empleo de herramientas como la inteligencia artificial para protegerse contra ciberataques, ciberterrorismo, crimen organizado.
    - Estimular la capacitación y desarrollo de personal en lo relacionado con el ciberespacio, bajo el marco de aplicación en la Antártida.
    - Con el establecimiento a futuro de una estación permanente en la Antártida por parte del Gobierno colombiano, se hace necesario desarrollar una infraestructura ciber- para distintas las labores científicas de carácter rutinario como para la protección de la información.

Referencias

Álvarez, C., & Namen, E. (2019). Geopolítica del Polo Sur: intereses y necesidades de Colombia en el Tratado de la Antártida. *Revista Científica José María Córdova, 17*(28), 721-748.

Avilés, J. (2005). *Las amenazas transnacionales en un mundo globalizado*. [Ponencia presentada en FAES] (13 de abril de 2005, pp. 1-12). Grupo de Estudios Estratégicos GEES.

Becerra, J., & León, I (2019). *La seguridad digital en el entorno de la fuerza pública diagnósticos y amenazas desde la gestión del riesgo*. DOI: https://doi.org/10.25062/9789585216549.02

Buck, S. (2013). T*he Global Commons. An introduction*. Routledge.

Cancelado, H. (2010). La Seguridad Internacional frente a las amenazas globales contemporáneas. *Jóvenes Investigadores, 2*.

Cardone, I. (2021). *Cuadernos de Política Exterior Argentina*. Centro de Estudios en Relaciones Internacionales de Rosario.

Comando General de las Fuerzas Militares. (2016). *Manual de ciberdefensa conjunta para las Fuerzas Militares*, [documento inédito]. Publicaciones de las Fuerzas Militares.

Comisión Colombiana del Océano (CCO) (2014). *Programa Antártico Colombiano*.

Conferencia de la Antártida (1959). *Tratado Antártico*. Conferencia de la Antártida.

Cornaglia, S., & Vercelli, A. (2017). La ciberdefensa y su regulación legal en Argentina (2006-2015). *Revista Latinoamericana de Estudios de Seguridad,* (20).

Delgadillo, V. (2018). El ciberespacio, un facilitador de riesgos. *Instituto de Investigaciones Estratégicas de la Armada de México*.

Departamento Nacional de Planeación (DNP) (2021). CONPES 3701. *Lineamientos de Política para la Ciberseguridad y la Ciberdefensa*.

Departamento Nacional de Planeación (DNP) (2016). CONPES 3854. *Política Nacional de Seguridad Digital*.

Departamento Nacional de Planeación (DNP) (2019). *Bases del Plan Nacional de Desarrollo 2018-2022*.

Echeverría, C. (2009). La innovación yihadista: propaganda, ciberterrorismo, armas y tácticas. *Grupo de Estudios Estratégicos GEES*.

Fontes, W. (2011). Uruguay en la Antártida: Una Visión Estratégica. *Centro de Altos Estudios Nacionales República Oriental de Uruguay*, 124-137.

Fuerza Aérea Colombiana (FAC) (2020). *Manual de doctrina básica aérea, espacial y ciberespacial.*

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

Fuerza Aérea Colombiana (FAC) (2020). *TOE código No. 4-03-08-20*. Subjefatura Estado Mayor de Estrategia y Planeación.

Galán, C. (2018). *Amenazas híbridas: nuevas herramientas para viejas aspiraciones*. Real Instituto Elcano Príncipe de Vergara.

Gobierno de España (2018). *PDC 01 (A) Doctrina para el empleo de las Fuerzas Armadas*. Ministerio de Defensa Español.

Gutiérrez, F. (2021). Características del ciberespacio que favorecen las actuales acciones de desinformación y decepción. *Instituto Español de Estudios Estratégicos,* (78).

Hermida, J., & Quintana, L. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. *Perspectivas en Psicología: Revista de Psicología y Ciencias Afines, 16*(2), 73-80.

International Telecommunication Union (ITU) (2020). *Global Cybersecurity Index*. https://n9.cl/ehuqs

Jarufe, J. (2022). Gobernanza en ciberseguridad: experiencia internacional. *Biblioteca del Congreso Nacional de Chile*, 25.

Jiménez, C. (2015). *El uso de ciberataques como herramienta de relaciones internacionales por parte de actores estatales: Los casos de Estados Unidos y Rusia.* Universidad Pontificia de Comillas.

Lazen, C. (2019). Las Reuniones Consultivas del Tratado Antártico: Desafíos del consenso ante los nuevos escenarios de negociación. Revista *Tribuna Internacional, 8*(15).

Lobato, L. (2017). La política brasileña de ciberseguridad como estrategia de liderazgo regional. *Revista Latinoamericana de Estudios de Seguridad*, 16.

López, J. (2012). La evaluación del conflicto hacia un nuevo escenario bélico. *El ciberespacio. Nuevo escenario de confrontación* (pp. 117-166).

Malekos, Z. (2022). Amenazas cibernéticas emergentes: ningún estado es una isla en el ciberespacio. *Real Clear Defense*. https://n9.cl/tyy22

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

Ministerio de Defensa Nacional de Uruguay. (2020). *Política de Defensa Nacional directivas periodo 2020-2025*.

Naciones Unidas, Asamblea General. (2004). *Seguimiento de los resultados de la Cumbre del Milenio A/59/565.*

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

Orozco, G. (2021). Una comparativa de los esquemas de ciberseguridad de China y Estados Unidos. *Revista OASIS*, (34), 107-126.

Pombo, L. (2015). Una Nueva Perspectiva en la Expresión del Poder. *Air and Space Power Journal,* 5.

Realpe, M., & Cano, J. (2020). Amenazas Cibernéticas a la Seguridad y Defensa nacionales. Reflexiones y perspectivas en Colombia. En *Seguridad Informática*. (X Congreso Iberoamericano, CIBSI). https://n9.cl/svbap

Reith, T. (2018). Blandir nuestras espadas aérea, espacial. Air and Space Power Journal, 57.

Rizzi, A. (2022, 30 de enero). ¿Quién tiene más ciberpoder? Una radiografía de las capacidades de EE. UU., China, Rusia y otras potencias. *El País*. https://n9.cl/cm0oi

Romero, O. (2019). Dimensiones, estrategias y alternativas de la integración autónoma para América Latina y el Caribe. Desafíos para el caso mexicano (2010-2015). Ediciones de la Noche.

Sampieri, F., Fernández, C., & Baptista, M. (2014). Definiciones de los enfoques cuantitativo y cualitativo, sus similitudes y diferencias. En *Metodología de la Investigación. McGraw Hill*.

Sánchez Acevedo, M., Becerra, J., León, I., Bohórquez Keeney, A., Páez Méndez, R., & Contreras Fernández, A. (2019). *La Seguridad en el Ciberespacio: Un desafío para Colombia*. Escuela Superior de Guerra.

Schreiber, C. (2019). *El Futuro de China y Rusia como Aliados en el Ciberespacio*. Grupo de Estudios en Seguridad Internacional (GESI). https://n9.cl/0xzpn

Secretaría del Tratado Antártico (1991). *Protocolo al Tratado Antártico sobre Protección del Medioambiente*.

Stel, E. (2014). *Seguridad y defensa del ciberespacio*. Dunken.

Oficina de las Naciones Unidas Contra la Droga y el Delito (UNODC) (2019). *Ciberespionaje*. https://n9.cl/eat2j

Voo, J., Hemani, I., Jones, S. DeSombre, W., Cassidy, D., & Schawarzenbach, A. (2020). *National Cyber Power Index 2020. Methodology and Analytical Considerations.* Belferd Center-Harvard Kennedy School.

Witker, I. (2015). *Entre una nueva guerra fría y el espíritu cooperativo: Características centrales del Programa Antártico Ruso*. Instituto Español de Estudios Estratégico. https://n9.cl/jc3vp

World Economic Forum (2022). *The Global Risks Report 2022*. https://n9.cl/b8eg8