VII Congreso del Instituto de Relaciones Internacionales

La Plata, 26, 27 y 28 de noviembre de 2014

Ciberdefensa: Una visión desde la UNASUR

Licenciada Candela Justribó

Resumen

El propósito de este artículo es poder reflexionar y analizar la posibilidad de unificar criterios y lineamientos en torno al rol del Instrumento Militar con respecto a la defensa en el ciberespacio dentro del ámbito de la Unión de Naciones Suramericanas (UNASUR), y su Consejo de Defensa Suramericano. A su vez, se considera la instalación y la subsiguiente consolidación de un plan de acción en conjunto que se lleve a cabo en la totalidad de los países integrantes de la UNASUR. A través de la recopilación de datos de fuentes primarias y secundarias se realizarán algunas observaciones sobre las diferencias, similitudes, obstáculos y facilidades que presenta el Consejo de Defensa Suramericano para establecer políticas en común, en pos de enfrentar los riesgos y amenazas que se presentan en un nuevo dominio operacional que representa el ciberespacio.

Palabras claves: UNASUR- Consejo de Defensa Suramericano- Fuerzas Armadas- Ciberdefensa

Introducción

Es de público conocimiento que el advenimiento de la tecnología en estos últimos años ha calado profundo en las relaciones interpersonales y en la agenda pública que tienen lugar dentro de la sociedad. Los continuos avances en materia de tecnologías de la información y de las comunicaciones ocasionan que éstas se inmiscuyan cada vez más en distintos ámbitos, ya sean a nivel global como local, incluyendo cuestiones relativas a lo que se entiende por defensa nacional y seguridad interior. De hecho, ya son conocidos los acontecimientos vinculados al espionaje ciberespacial y a los ataques cibernéticos, registrando como casos emblemáticos los ciberataques sufridos por instituciones de Estonia en el año 2007, el arma virtual *Stuxnet*, o las actividades de ciberespionaje desarrolladas por la National Security Agency (NSA) de los Estados Unidos y difundidas por su ex agente Edward Snowden.

Los eventos antes mencionados causaron que, si antes los asuntos relativos al ciberespacio fueran mirados con desinterés, después de ellos, los Estados- nación comenzarán a depositar en estos temas una mayor dedicación y esfuerzo en discutir qué es lo que realmente implica este nuevo dominio estratégico, si puede ser definido como un nuevo escenario militar, y en el caso de que lo fuera, qué papel cumple el Instrumento Militar de cada uno de los Estados- Nación, lo que da lugar a una serie de alternativas y planes de acción muy diversos entre sí.

En el contexto suramericano, la creación de la Unión de Naciones Suramericanas (UNASUR) y de su Consejo de Defensa Suramericano (CDS) en el año 2008, organización de defensa regional, significaron la continuación del proceso de integración y de la relevancia en cuestiones tales como la cooperación, la complementariedad y la confluencia; lo que implica un fortalecimiento en las medidas de confianza y el abandono de hipótesis de conflicto, asunto que había alcanzado su auge alrededor de la década del setenta, donde la gran parte de los países de la región se encontraba bajo la Doctrina de Seguridad Nacional, pregonada por los Estados Unidos.

Después de la redemocratización de los países de América del Sur, los diferentes dirigentes que ocuparon los sillones presidenciales comenzaron a desarrollar acuerdos bilaterales y diversos mecanismos de cooperación en distintas áreas, llegando, al fin, a la institucionalización de esa integración en la UNASUR, y en particular en el CDS, que en palabras de Alfredo Forti, contribuyen a

"afianzar Suramérica como zona de paz y consolidar una identidad suramericana de Defensa" (2009: 71).

El planteamiento que define al Consejo de Defensa Suramericano como un "órgano de consulta, cooperación y coordinación en materia de defensa" (Estatuto del Consejo de Defensa Suramericano, 2008) implica también avanzar sobre una visión compartida sobre los diferentes tópicos que abarca la defensa nacional y, por ende, la seguridad regional. Frente a las nuevas preocupaciones que el ciberespacio acarrea con él, cabe preguntarse qué rol cumple el Consejo de Defensa Suramericano a partir de las diferentes concepciones que tiene cada país miembro sobre las esferas de defensa nacional y seguridad interior, las políticas de defensa que llevan a cabo y el concepto que poseen de la denominada ciberdefensa y las acciones desplegadas, ya sea por el instrumento militar con el que cuentan cada uno de ellos o por otro organismo responsable de ello.

Para ello, en primer lugar, se desarrollarán los avances hechos en la materia de ciberdefensa por el Consejo de Defensa Suramericano y que es lo que significan cada uno de ellos. En segundo lugar, se hará una aproximación a los diferentes enfoques que hacen sobre defensa nacional y seguridad interior tres países miembros de la UNASUR como son Argentina, Brasil y Colombia, los cuales presentan marcos legislativos, políticos y doctrinarios disímiles, y que, a partir de ello, también, presentarán diferentes avances en torno a las acciones realizadas a favor de la ciberdefensa de cada uno de ellos, y que por ello resultan representativos de las posturas que pueden identificarse y que actualmente conviven al interior del Consejo de Defensa Suramericano. Por último, se intentará responder cuales son los obstáculos y las ventajas para poder desarrollar una política de ciberdefensa en común y que garantice la defensa de los Estados- nación que conforman la organización regional en torno a la defensa.

La ciberdefensa en el marco del Consejo de Defensa Suramericano

Cada año, el CDS impulsa la realización de un plan de acción que, en general, tendrá como ejes cuatro puntos, entre los cuales se desarrollan Políticas de Defensa, Cooperación Militar, Acciones Humanitarias y Operaciones de Paz, Industria y Tecnología y Formación y Capacitación.

Ante ello, en el año 2012, se aprobó el Plan de Acción correspondiente a ese año, donde en el eje de "Políticas de Defensa" abarca, en su punto 1.F, la "conformación de un Grupo de Trabajo para evaluar

la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa", siendo responsable la República del Perú. De esta manera, ya se comenzaban a hacer intentos en el marco de la organización regional en pos de darle mayor relevancia y un mayor dimensionamiento a la problemática que representa el tema ciberdefensa y un mayor alcance en las políticas de defensa que implementa el Consejo de Defensa Suramericano.

En forma complementaria y coherente, al año siguiente, el Plan de Acción del 2013, también en el eje de "Políticas de Defensa", postula como actividad a desarrollar el mantenimiento del grupo de trabajo creado el año anterior a fin de que exista la posibilidad de "establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa".

No obstante, el puntapié principal para comenzar a desarrollar de manera más fehaciente, profunda y constante, estrategias defensivas en lo que respecta al ciberespacio para implementar a nivel regional se dio con la I Declaración de Paramaribo, en la República de Suriname, el 30 de agosto del año 2013, fecha cercana a la confirmación de actividades de ciberespionaje sobre el gobierno de Brasil por parte de Estados Unidos. En la misma, los Jefes y Jefas de Estado y de Gobierno de los países miembros instruyen

> "al Consejo de Defensa Suramericano y al COSIPLAN a evaluar la cooperación con otros consejos ministeriales competente y avanzar en sus respectivos proyectos de defensa cibernética y la interconexión entre redes de fibra óptica en nuestros países con vistas a tornar más seguras nuestras telecomunicaciones. Promover el desarrollo de tecnologías regionales y la inclusión digital. Saluda el interés del MERCOSUR en estrechar su coordinación con la UNASUR sobre esos temas e instruye al CDS y al COSIPLAN a trabajar regularmente en coordinación con el recién creado Grupo de Trabajo de MERCOSUR, responsable por asuntos de telecomunicaciones, y a enviar un informe con las recomendaciones sobre posibles avances en la materia durante la Reunión Ordinaria de la UNASUR"

Así es como resultado de lo antedicho, en la V Reunión Ordinario del Consejo de Defensa Suramericano y en su correspondiente Declaración de Paramaribo, las Ministras y Ministros de Defensa retoman lo expuesto en la Reunión de Jefes y Jefas de Estado y revalidan lo anunciado por ellos en torno a las amenazas cibernéticas e informáticas. En este sentido, ratificaron la necesidad de avanzar en las coordinaciones regionales en materia de ciberdefensa y aprobaron el Plan de Acción del año 2014, que resulta relevante, ya que, por primera vez se incluye una actividad didáctica concerniente

a la defensa cibernética y respondiendo a la instrucción de la I Declaración de Paramaribo, siendo ésta un Seminario Regional de Ciberdefensa.

El mismo se celebró en la ciudad de Buenos Aires, República Argentina, entre los días 14 al 16 de mayo, y contó con la presencia de personalidades de diferentes organismos, tanto argentinos como de los países de la región, y se expusieron temas en torno a las infraestructuras críticas y seguridad de la información, a los ecosistemas de computación en la nube, a la seguridad de las comunicaciones y a las tecnologías de la información y de las comunicaciones, entre otros.

Paralelamente a este seminario, y cerrado al público, se conformó la tercera reunión del Grupo de Trabajo de Ciberdefensa que se conforma en el marco del Consejo de Defensa Suramericano, el cual, por consenso, anunció la necesidad de desarrollar cuatro puntos básicos:

1. "Crear un foro regional del Grupo de Trabajo de Ciberdefensa de los Estados Miembros, a fin de intercambiar conocimientos, experiencias y procedimientos de solución.
2. Establecer una red de contactos de autoridades competentes para el intercambio de información y colaboración de manera permanente.
3. Definir la plataforma y procedimientos de comunicaciones de la red de contactos.
4. Profundizar y sistematizar la reflexión sobre definiciones conceptuales de ciberdefensa y ciberseguridad(Declaración de Cartagena del Consejo de Defensa Suramericano, 2014)".

Con estas iniciativas, el grupo de trabajo ya no se limita a reuniones esporádicas de intercambio de información, sino que con la creación y el establecimiento de un foro regional y de una red de contactos, lo que se busca es poder tornar más constante la actividad y los mecanismos instalados para poder combatir las amenazas cibernéticas e informáticas.

Asimismo, en la misma Declaración de Cartagena se hace alusión a los avances que se obtuvieron alrededor de estos cuatro puntos, anunciando la difusión de la red de contactos y el inicio de las coordinaciones para las pruebas de comunicación para crear una plataforma de comunicación mediante correo electrónico y telefonía fija y móvil. También, y en relación al Foro Regional, el grupo de trabajo comenzó a acordar, en forma particular, con Argentina el empleo de la plataforma UNACERT. Por su parte, otro avance significativo fue la solicitud a los países miembros de la terminología empleada por cada país con el objetivo de elaborar, en colaboración con el Centro de Estudios Estratégicos para la Defensa, un documento en el que se pueda exponer definiciones conceptuales y términos relacionados

a la ciberdefensa y a la ciberseguridad, de manera de poder unificarlos a nivel regional, lo que representaría un gran avance ya que, hasta el momento, se carece de un consenso académico y político de lo que significan estos dos conceptos.

Por su parte, también se encuentran acuerdos, que se dan en el marco de la Unión de Naciones Suramericanas y de su Consejo de Defensa Suramericano, entre Brasil y Argentina y Chile. En primer lugar, en septiembre del año 2013, se celebró una reunión bilateral en Buenos Aires con los Ministros de Defensa Agustín Rossi (Argentina) y Celso Amorim (Brasil) en la cual se propuso la constitución de un subgrupo de trabajo bilateral con la necesidad de continuar impulsando la cooperación en lo que es ciberdefensa. En un segundo encuentro, realizado en noviembre del mismo año, se ratifica la necesidad de colaborar en el área de defensa cibernética, con el fin de fortalecer la estrategia defensiva. Así, se acordó una agenda de trabajo que abarca las áreas de capacitación (con la creación de vacantes para militares argentinos en cursos de oficiales y suboficiales en Brasil, vacantes en una maestría de seguridad de la información y criptografía), de métodos y sistemas tecnológicos, de doctrina combinada, de intercambio de integrantes de los CSIRT – *computer security incident response team*- y de investigación científica, materializando las tentativas de cooperación en lo que es la asociación estratégica entre Brasil y Argentina.

En segundo lugar, y recientemente, la República de Chile junto con la República Federativa del Brasil, firmaron un acuerdo a nivel ministerial en el que los titulares de la cartera detectaron diversas áreas de cooperación, entre las cuales se encuentra la industria militar, aérea y naval, operaciones de paz, intercambios académicos, y el tema que atañe a este artículo, la ciberdefensa, para que el Grupo de Trabajo Bilateral elabore planes de implementación.

De este modo, se pueden ver grandes avances en materia de defensa cibernética en lo que incumbe al Consejo de Defensa Suramericano. Sin embargo, las diferencias relativas al marco normativo y doctrinario de cada Sistema de Defensa Nacional de los países miembros se caracterizan por contar con bastantes disimilitudes en cuanto a lo que entienden por defensa nacional y seguridad interior, lo que desencadenará en entender los conceptos de ciberdefensa y ciberseguridad de diversas formas.

Estudios de caso: Argentina, Brasil y Colombia

A continuación, se hará referencia a la legislación y a la doctrina que rige, estructura y domina el Sistema de Defensa Nacional de tres países miembros del Consejo de Defensa Suramericano: Argentina, Brasil y Colombia. Estos Estados- nación, como ya se ha mencionado anteriormente, presentan características muy diferentes en lo que se refiere al rol del Instrumento Militar y a su doctrina, y por ende, también las presentaran en lo que atañe a la defensa cibernética o ciberseguridad. Al mismo tiempo, resultan representativos de los avances que se están realizando en materia de ciberdefensa en la región.

Argentina

A partir de los antecedentes históricos que presenta la República Argentina, uno de los principales liminares (Eissa: 2013) que presenta la política de defensa es la distinción de las esferas entre defensa nacional y seguridad interior. En comparación con otros países pertenecientes a la región, la distinción entre los aspectos de defensa y seguridad comenzó con la sanción de la Ley 23.554 de la Defensa Nacional, la cual define a la defensa como "la integración y acción coordinada de todas las fuerzas de la Nación para la solución de aquellos conflictos que requieran el empleo de las Fuerzas Armadas, en forma disuasiva o efectiva, para enfrentar las agresiones de origen externo".

Sin embargo, recién en el año 1991 con la creación de la Ley 24.059 de Seguridad Interior se estableció que las Fuerzas Armadas participarían en cuestiones de seguridad como misión complementaria y en casos eventuales, poniendo a disposición sus servicios de veterinaria, arsenales, sanidad, intendencia, construcciones y transporte y se define, en su artículo 2, a la seguridad interior como "a la situación de hecho basada en el derecho en la cual se encuentran resguardadas la libertad, la vida y el patrimonio de los habitantes, sus derechos y garantías y la plena vigencia de las instituciones del sistema representativo, republicano y federal que establece la Constitución Nacional".

Consecutivamente, en el año 2006, se reglamentó la Ley de Defensa Nacional mediante el Decreto 727 del año 2006, especificando que las Fuerzas Armadas tendrán el deber de "conjurar y repeler cualquier agresión externa perpetrada por Fuerzas Armadas de otro/s Estado/s", es decir, contra cualquier agresión externa militar estatal, con el objetivo de defender los intereses vitales de la Nación, como son la soberanía, la integridad territorial, la independencia y la protección de la vida y la libertad de sus habitantes. Así, tomando el concepto de agresión de la Resolución 3314 de la Organización de Naciones Unidas para establecer la misión principal del Instrumento Militar, se establece el rechazo

hacia cualquier intento que pretenda extender la utilización de las Fuerzas Armadas contra las llamadas "nuevas amenazas"[1], impidiendo que sus "aspectos doctrinario, de planeamiento y adiestramiento, así como también la producción de inteligencia" se estructuren en base a estas problemáticas.

Complementariamente, el Decreto N° 1691 del mismo año aprueba la Directiva de Organización y Funcionamiento de las Fuerzas Armadas que especifica sus misiones complementarias, entre las cuales se encuentran la participación en operaciones de mantenimiento de la paz bajo mandato de las Naciones Unidas, la participación en la conformación de un Sistema de Defensa Subregional, la participación en apoyo a países amigos y/o a la comunidad frente a desastres naturales y/o antrópicos, y por último, la participación en operaciones de seguridad interior en los casos en que se brinde apoyo logístico, en el restablecimiento del orden frente a un ataque dentro de la jurisdicción militar, y en operaciones de empleo del combate, por disposición de la Presidenta de la Nación y previa declaración del estado de sitio, "para el restablecimiento de la normal situación de seguridad interior en aquellos casos excepcionales en que el sistema de seguridad interior resulte insuficiente a criterio del Presidente de la Nación".

Así, se desprende que los criterios para diferenciar la ciberdefensa de la ciberseguridad, y las estrategias alrededor de estos conceptos, derivarán de la misma distinción que se hace normativamente de la defensa nacional y la seguridad interior. Argentina, si bien ya tiene una política de seguridad definida con su respectivo organismo responsable de ello, recientemente comenzó a desarrollar iniciativas vinculadas a la defensa cibernética.

En referencia a la ciberseguridad, el país, en el año 2003, a través del Decreto 1028/2003 le otorga a la Oficina Nacional de Tecnologías de la Información (ONTI), la responsabilidad de entender y regular los lineamientos en referencia a la protección de datos y a la seguridad y privacidad de la información digital, dependiendo de la Jefatura de Gabinete de Ministros de la Nación. Así, surgió la necesidad de establecer y de unificar parámetros para elaborar una política nacional y mecanismos de seguridad para instalar en las agencias de la Administración Pública Nacional. La decisión administrativa N° 669 del año 2004 significó el primer gran avance en materia de seguridad de la información, estableciendo la "Política de Seguridad Modelo", la cual fue actualizada mediante la Disposición ONTI N° 3/2013.

[1] Para desarrollar el tema de nuevas amenazas, ver DERGHOUGASSIAN, K. (2008). *Las nuevas amenazas en la perspectiva estratégica del riesgo: una visión crítica*, en Construyendo Roles. Democracia y Fuerzas Armadas. Buenos Aires: CELS. Págs 37-41.

Al mismo tiempo, esta agencia estatal lleva a cabo diferentes productos, entre los que se encuentra el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC)[2] que presenta el objetivo de incentivar la creación y la adopción de un programa regulatorio que preserve las infraestructuras estratégicas de la información del Estado.

Por otro lado, en el ámbito del Ministerio de Defensa y al ser caracterizado como un nuevo dominio estratégico, el ciberespacio comenzó a tener más relevancia dentro de las políticas y estrategias de esta cartera, derivando en la aprobación de un compendio de resoluciones a nivel ministerial.

Una de las primeras señales de los avances de la jurisdicción defensa en referencia al ciberespacio, se dio con la Resolución del Ministerio de Defensa N° 364 del año 2006, la cual crea el Comité de Seguridad de la Información, que debe su origen a la Decisión Administrativa N° 669/ 2004, plegándose a lo estipulado por la ONTI sobre la "Política de seguridad de la información modelo".

Posteriormente, la Resolución N° 385 del año 2013 estableció la creación de la Unidad de Coordinación de Ciberdefensa, dependiente de la Jefatura de Gabinete de Asesores del Ministerio de Defensa. Este mismo es el responsable de precisar las funciones e integración de dicha unidad, uniendo en una sola agencia administrativa la coordinación de la política referente a la ciberdefensa en el ámbito de la jurisdicción, en pos de "generar mecanismos integrados de respuesta para la toma de decisiones". Así, esta unidad estará compuesta por representantes de cada área del Ministerio de Defensa, del Estado Mayor Conjunto de las Fuerzas Armadas y de los Estados Mayores Generales de las Fuerzas Armadas.

Con la aparición de la Resolución N° 350 del año 2014, por primera vez se incorpora al Instrumento Militar como integrante de la estrategia de defensa cibernética nacional. En este sentido, se instruye al Jefe del Estado Mayor Conjunto de las Fuerzas Armadas para que,

> "disponga las medidas necesarias a los efectos de desarrollar capacidades militares para realizar operaciones de ciberdefensa, a los efectos de únicamente garantizar la defensa contra aquellos ciberataques que pretendan obstaculizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal" y contra aquellos ciberataques "que dirigidos a afectar los objetivos de valor estratégico que el Ministerio de Defensa establezca expresamente".

[2] Resolución N° 580/2011

Al mismo tiempo, se le instruye para que elabore un plan de desarrollo de capacidades de ciberdefensa y la doctrina básica conjunta, derivada y de procedimientos de Ciberdefensa, los cuales deberán ser elevados al Ministerio de Defensa.

Complementariamente, mediante la Resolución N° 351 del corriente año, también del Ministerio de Defensa, se crea el Comando Conjunto de Ciberdefensa, dependiente orgánica, funcional y operacionalmente del Estado Mayor Conjunto de las Fuerzas Armadas que tendrá como función desarrollar las capacidades para ser capaz de garantizar las operaciones militares del Instrumento Militar de la Defensa Nacional en cumplimiento de su misión principal y de acuerdo a los lineamientos establecidos en el planeamiento estratégico militar. Además, define al ciberespacio como un dominio transversal, de esta manera se expone la lógica de crear un Comando Conjunto: al ser un dominio que atraviesa a los escenarios más tradicionales de combate – aire, agua, y tierra- es necesario que la agencia responsable de elaborar y desarrollar capacidades de ciberdefensa sea conjunto e integrado, es decir, que esté formado por representantes de las tres Fuerzas Armadas.

Vale destacar que al ser el Comando Conjunto de Ciberdefensa el encargado de la ciberdefensa, ésta última pasa a ser un concepto operacional, por ende, no debe reducirse a la inteligencia, a la seguridad de datos o a las comunicaciones, sino que debe estar constantemente orientada a la misión principal del Instrumento Militar.

Brasil

La defensa nacional en la República Federativa del Brasil está íntimamente ligada a la estrategia de desarrollo nacional (Estrategia de Defensa Nacional, 2008), es decir, según esta postura el desarrollo nacional será fuerte si se tiene una defensa fuerte que se estribe en la independencia nacional, la cual se apoya en tres ejes fundamentales: por la movilización de recursos físicos, humanos y económicos; por la capacitación tecnológica autónoma, y por último, por la democratización de oportunidades educativas y económicas (2008: 09).

Complementaria a esta idea, una de las directrices que reciben las Fuerzas Armadas por parte de esta Estrategia de Defensa Nacional elaborada y aprobada por el Nivel Estratégico Nacional es la de promover y desarrollar tres sectores de importancia estratégica: el espacial, el cibernético y el nuclear (2008: 12). Con respecto al eje cibernético, la directriz ordena que las capacidades militares relativas a

la ciberdefensa se dirijan a los ámbitos industrial, educativo y militar. Como prioridad, se incluirán las tecnologías de la información entre todos los contingentes de las Fuerzas Armadas para garantizar su actuación en red. De esta manera y bajo esta concepción, el ciberespacio representaría un dominio operacional diferente a los ambientes operacionales tradicionales, contrario a lo que postula Argentina.

En el año 2009, el Ministerio de Defensa, por medio de la Directriz Ministerial N° 14, designó para cada sector estratégico una fuerza responsable, con el fin de lograr una coordinación de acciones entre los mencionados sectores. Entonces, la Marina pasó a ser la encargada del área correspondiente a las actividades nucleares, la Fuerza Aérea se ocuparía del ámbito espacial, y el Ejército Brasilero del ambiente cibernético.

A partir de la Ley Complementar N° 136 del año 2010, se establece que a partir de año 2012, el Poder Ejecutivo remitiría al Congreso Nacional, entre períodos de cuatro años la Política de Defensa Nacional, la Estrategia de Defensa Nacional y el Libro Blanco de la Defensa Nacional. El primer documento enuncia explícitamente que se entiende por defensa y seguridad. En primer lugar, el marco normativo de Brasil considera que la defensa es el conjunto de medidas y acciones del Estado, con énfasis en el campo militar" (2012: 02), a fin de proteger el territorio, la soberanía y los intereses nacionales contra amenazas externas, ya sean potenciales o manifiestas.

Mientras tanto, la seguridad es definida como la "condición que permite al país preservar su soberanía e integridad territorial, promover sus intereses nacionales, libre de presiones y amenazas y garantizar a los ciudadanos el ejercicio de sus derechos y deberes constitucionales" (2012:02).

De estas dos definiciones, se desprenden la misión principal y las misiones subsidiarias del Instrumento Militar. Las Fuerzas Armadas deben su estructura y su diseño a la "defensa de la patria y a la garantía de los poderes constitucionales y, por iniciativa de ellos, a la ley y al orden" (Constitución de la República, Art. 142). Asimismo, se identifican cuatro tareas subsidiarias, entre las cuales se encuentran las operaciones de paz, la cooperación en el desarrollo nacional y la defensa civil, participación en campañas institucionales de utilidad pública o interés social, la participación, por medio de medidas preventivas y represivas en el control de acciones fronterizas, en el mar y en aguas interiores, efectuando entre otras acciones el patrullaje, detención por delito, y revista de personas, de vehículos

terrestres, embarcaciones y aeronaves.[3] Esta noción de la misión principal y de las misiones subsidiarias del Instrumento castrense refleja la concepción que tiene el país si de defensa y seguridad se habla. Los límites entre ambas esferas se encuentras desfigurados y si bien, las Fuerzas Armadas son responsables de tareas con similares características que en otros países de la región, también se debe admitir que éstas adquieren cada vez más protagonismo dentro de las acciones llevadas a cabo como respuesta a disturbios sociales o ante las ya mencionadas, nuevas amenazas a través de la denominada, y ya conocida, Policía Militar.

En el ámbito de la defensa cibernética, a partir del 2010, se comenzó a hablar del Centro de Defensa Cibernética, dependiente del Ejército Brasilero y que complementa, mediante las acciones destinadas, a otras organizaciones gubernamentales ya existentes en pos de brindar confiabilidad, disponibilidad, integridad y autenticidad en lo que es tráfico de datos. El Centro de Defensa cibernética tiene el propósito de mejorar la capacitación de los recursos humanos, de actualizar la doctrina, de fortalecer la seguridad, de responder ante incidentes de redes y de proteger frente ataques cibernéticos (Libro Blanco de la Defensa Nacional, 2012).

Por otro lado, la Estrategia de Defensa Nacional del año 2012 recalca, una vez más, la importancia y la necesidad de continuar desarrollando el sector cibernético detentado por las Fuerzas Armadas. De esta manera, precisa las prioridades a las que el Instrumento Militar deberá dedicarle más atención y esfuerzo en materia de defensa cibernética.

La primera de ellas hace hincapié en el fortalecimiento del Centro de Defensa Cibernética para alcanzar la capacidad de evolucionar hacia un Comando de Defensa Cibernética de las Fuerzas Armadas. En segundo lugar, se buscará mejorar la seguridad de la información y de las comunicaciones, específicamente, en lo vinculado a la certificaciones digital de las Infraestructuras claves y públicas de la Defensa. Consiguientemente, otro de los objetivos es fomentar la investigación científica orientada al área de defensa cibernética, incluyendo a la comunidad nacional e internacional, recurriendo a la cooperación e integración con otros Ministerios que, por sus competencias, puedan asistir, desde diferentes visiones, con el objetivo. Además, se sugiere desarrollar sistemas computacionales de uso

[3] Establecidas por la Ley Complementaria N° 97 y su reforma, Ley Complementaria N° 136- Art 15 y 16.

dual y tecnologías que permitan el planeamiento y la ejecución de la Defensa Cibernética en el ámbito del Ministerio de Defensa y que contribuyan con la seguridad cibernética nacional, entre otras directrices que se deben priorizar.

Ahora bien, a nivel político, Brasil ya presenta una estructura básica en lo concerniente a las áreas de seguridad cibernética y de defensa cibernética (como ya se nombró al Centro de Defensa Cibernético). Otras organizaciones públicas importantes vinculadas a la materia son la Casa Civil de la Presidencia de la República y el Ministerio de Justicia, en particular, la Policía Federal. En palabras de Raphael Mandarino Junior, la seguridad cibernética "se caracteriza, cada vez más, como una función estratégica de Estado, y por lo tanto, se hace esencial la manutención y preservación de las infraestructuras críticas del país, tales como la energía, transporte, telecomunicaciones, agua, finanzas, información, y otras (Mandarino, 2010: 13)"[4].

Esta concepción deriva del accionar conjunto que se detecta en el ámbito de la cibernética en Brasil por parte de diferentes organismos de distinta índole, que incluyen al Consejo de Defensa Nacional, a la Cámara de Relaciones Exteriores y Defensa Nacional, al Consejo de Gobierno y a su Gabinete de Seguridad Institucional de la Presidencia de la República (GSI/ PR), la cual cumple con los roles de ser Secretaria Ejecutiva del citado Consejo y de detentar la Presidencia de la Cámara. Otra atribución del GSI/PR es la coordinación de actividades de inteligencia federal y de la seguridad de la información, contando al interior de su estructura con un Comité Gestor de Seguridad de la Información, grupos de trabajo de Seguridad de las Infraestructuras Criticas, en las áreas de energía, telecomunicaciones, transportes, finanzas y adquisición de agua, el Grupo de Trabajo de Seguridad de las Infraestructuras Críticas de la Información, el Grupo Técnico de Seguridad Cibernética y el Grupo Técnico de Criptografía.

Asimismo, otro mecanismo de seguridad importante aparte de las instituciones nombradas, es la Política de Seguridad de la Información en las agencias pertenecientes a la Administración Pública Federal. Cabe destacar también la presencia de la Red Nacional de Seguridad de la Información y Criptografía (RENASIC), que cumple con sus responsabilidades de funcionar como el núcleo de intercambio de información entre investigadores sobre el tema bajo la coordinación de la GSI/PR.

[4] Traducción propia.

Vale decir, que además, el GSI/PR es la encargada de elaborar las actividades que resulten relevantes para cumplir con las responsabilidades del Consejo de Defensa Nacional y la Cámara de Relaciones Exteriores y Defensa Nacional, entidades que cuentan con cierta independencia dentro del sector cibernético en los campos de decisiones estratégicas y de la formulación de las políticas públicas y de lineamientos y criterios a tener en cuenta en la materia.

Por lo tanto, resulta primordial que las funciones de coordinación y de integración se mantengan bajo un órgano de la Presidencia, tal como acontece con el GSI/PR, lo que, indefectiblemente, tiene sus efectos sobre las actividades de defensa cibernética, que si bien se encuentran directamente ligadas a la jurisdicción del Ministerio de Defensa y de las Fuerzas Armadas, necesitan de la relación establecida con el Consejo de Defensa Nacional y de la Cámara de Relaciones Exteriores y Defensa Nacional para el mantenimiento de la coherencia con las acciones desplegadas por otras instancias públicas y privadas de interés.

Expuesto el marco normativo y doctrinario adoptado por Brasil, se explica el concepto de defensa cibernética y de seguridad informática que utilizan para desplegar y desarrollar estrategias ciberdefensivas. Al aparecer la defensa nacional y la seguridad interior poco limitados, y por cierto, resultando hasta complementarios uno con el otro, se entiende que en materia de políticas de ciberseguridad y de defensa cibernética, los organismos responsables de ellas también se complementaran. Así, lo que caracteriza el trabajo llevado a cabo por los diferentes instrumentos designados para ello, es la actividad en conjunto, sin precisar áreas especializadas para tal fin.

Colombia

En la República de Colombia, por los acontecimientos ya conocidos, dados por la fusión entre el narcotráfico, los grupos guerrilleros y sus actividades terroristas que conviven al interior del territorio nacional, las circunstancias que dan forma al Sistema de Defensa Nacional colombiano son totalmente distintas a los sistemas pertenecientes a los países precedentemente desarrollados.

A través de una serie de tres documentos, denominados como “Política de Consolidación de la Seguridad Democrática (2006- 2010)”, “Política Integral de Seguridad y Defensa para la Prosperidad (2011)” y “Política Nacional de Defensa de la Libertad Personal (2011- 2014)” que expresan y reúnen

las políticas implementadas en el campo de la defensa y la visión que se tiene sobre el rol de las Fuerzas Armadas a partir de ellas.

En ellos, la defensa y seguridad como una unidad cumplen un rol preponderante en el objetivo nacional que es "alcanzar condiciones de seguridad óptimas para garantizar la prosperidad democrática y el progreso nacional" (RESDAL, 2012: 169). Siendo así, se considera necesario que exista un "accionar integrado y creciente de las otras instituciones del Estado y de la comunidad" (Política Integral de Seguridad y Defensa para la Prosperidad, 2011: 21), y como propósito superior se apunta a "la gobernabilidad democrática, la prosperidad colectiva y la erradicación de la violencia, mediante el ejercicio de la seguridad y la defensa, la aplicación adecuada y focalizada de la fuerza y el desarrollo de capacidades mínimas disuasivas" (Política Integral de Seguridad y Defensa para la Prosperidad, 2011: 31).

En particular, la Política Integral de Seguridad y Defensa para la Prosperidad, al igual que la Política Nacional de Defensa de la Libertad Personal, presentan seis objetivos y estrategias sectoriales a desarrollar promovidos por el Ministerio de Defensa Nacional que presentan como objetivos alcanzar un equilibrio entre seguridad interna y disuasión interna (Política Integral de Seguridad y Defensa para la Prosperidad, 2011), lo que implica una estructura de fuerza polivalente e interoperable.

De esta manera, las estrategias y objetivos sectoriales se identifican con el alcance de un mínimo histórico la producción nacional de narcóticos, con la desarticular los grupos al margen de la ley y crear condiciones suficientes de seguridad para la consolidación, con la creación de condiciones de seguridad para la convivencia ciudadana, con el avance hacia un sistema de capacidades disuasivas creíble, integrado e interoperable – objetivo que contiene la adopción de un programa de ciberseguridad y ciberdefensa-, con la contribución a la atención oportuna a desastres naturales y catástrofes y con el fortalecimiento la institucionalidad y el bienestar del sector seguridad y defensa.

Las Fuerzas Militares, de este modo, presentarán como misión principal la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional (RESDAL, 2012, 170). Además, el máximo nivel estratégico militar es el Comando General de las Fuerzas Armadas, que conducirá las operaciones militares que se orienten a "defender la soberanía, la independencia, la integridad territorial y la derrota de la amenaza, para contribuir a generar un ambiente de paz, seguridad y desarrollo garantizando el orden constitucional de la nación" (RESDAL, 2012: 170).

Esta concepción que se le otorga a la defensa y a la seguridad resulta en un diseño y una estructura que abarcan amenazas, no sólo de tipo externo, sino también, aquellas que atenten contra la libertad personal. Puesto que, en general, estas amenazas se dan a partir de la acción de grupos fuera de la ley y del orden, se afirma que las agencias estatales deben trabajar en conjunto, ajustando su respuesta dependiendo de la naturaleza y la orden del agresor. A partir de lo expuesto en la Política de Defensa de la Libertad Personal, "el Estado buscará actuar de forma transversal enfocando recursos de diverso tipo para provocar una reducción radical de los atentados contra la libertad personal utilizando de forma convergente distintas herramientas" (2011: 16).

En referencia a las acciones vinculadas al programa de ciberseguridad y ciberdefensa, establecido a favor de lo dispuesto por el objetivo y estrategia sectorial número cuatro (Avance hacia capacidades disuasivas), a partir de la enunciación del ciberespacio como "la red interdependiente de infraestructuras de tecnología de la información, que incluye Internet y otras redes de telecomunicaciones, sistemas computacionales, procesadores integrados y controladores de industrias críticas" (Dirección de Estudios Sectoriales *et al*, 2009: 1), el origen de dicho programa se remonta al año 2005.

El mismo considera que el Estado debe proteger su infraestructura cibernética, dado que cualquier agresión o detrimento de capacidades en ella puede causar daños al ciudadano, y otras áreas como son la gubernamental, la comercial o de finanzas, y la industrial. En consecuencia, y en el marco de este programa de estrategias ciberdefensivas y de ciberseguridad, una de las primeras iniciativas en las que se trabajó fue en un grupo de trabajo interagencial dirigido por el Ministerio de Relaciones Exteriores a fin de poder estudiar, analizar y evaluar los fenómenos al interior de lo que se considera ciberespacio. En consonancia con esta labor, el Ministerio de Tecnología de la Información y de las Comunicaciones realizó estudios que dieron como conclusión la ausencia de políticas contra la intrusión informática en Colombia, y que a su vez, resultaron en la decisión de que el Ministerio de Defensa sea el responsable de liderar las problemáticas características de la ciberdefensa y la ciberseguridad.

Por otro lado, se resolvió crear, en el marco de la política de ciberdefensa y ciberseguridad aprobado por el Consejo Nacional de Política Económica y Social, en el año 2011, el colCERT (*Equipo de Respuesta a Emergencias Informáticas de Colombia),* que es el órgano público responsable, a escala nacional, de crear un marco de regulación y de coordinación de las acciones que resulten necesarias

para mantener la protección de las infraestructuras críticas pertenecientes al país frente a posibles ataques cibernéticos que puedan llegar a afectar la defensa y la seguridad nacional. Está constituido por integrantes del Ministerio de Defensa.

Paralelamente, se crean dos entidades más que complementarán al colCERT: el Comando Conjunto Cibernético y el Centro Cibernético Policial. El primero de ellos es el primer órgano militar vinculado al dominio ciberespacio. Conformado por integrantes de las tres Fuerzas Armadas, es el encargado de garantizar y salvaguardar los intereses nacionales en el ciberespacio, es decir, protegerá las infraestructuras críticas del Estado y del sector defensa, ante cualquier amenaza o ataque cibernéticos que puedan surgir. A partir del Documento CONPES 3701, que devela los lineamientos a seguir en materia de ciberseguridad y ciberdefensa, se destacan las siguientes funciones del Comando:

> "Fortalecer las capacidades técnicas y operativas del país que permitan afrontar las amenazas informáticas y los ataques cibernéticos, a través de la ejecución de medidas de defensa a nivel de hardware y/o software y la implementación de protocolos de ciberdefensa; defender la infraestructura crítica y minimizar los riesgos informáticos asociados con la información estratégica del país, así como reforzar la protección de los sistemas informáticos de la Fuerza Pública de Colombia; desarrollar capacidades de neutralización y reacción ante incidentes informáticos, que atenten contra la Seguridad y Defensa Nacional (2011:25)".

Adicionalmente, se encuentra, en el ámbito de la Policía Nacional, el Centro Cibernético Policial, que cumple con tareas y actividades dedicadas a la atención, prevención e investigación y dará apoyo a la judicialización de los delitos informáticos. Además, atenderá los lineamientos nacionales de ciberseguridad y trabajará bajo el mandato del colCERT Para ello, operativamente, contará con un Comando de Atención Inmediata Virtual, para recoger denuncias de los ciudadanos.

Al frente de estas tres organizaciones se consolidó la imagen de una Comisión Intersectorial, encabezada por el Presidente de la República y compuesta por el Ministro de Defensa Nacional, el Ministro de Tecnologías de Información y Comunicaciones, el Director del Departamento Administrativo de Seguridad, el Director de Planeación Nacional y el Coordinador del colCERT, y presenta como rol el "fijar la visión estratégica de la gestión de la información, así como de establecer los lineamientos de política respecto de la gestión de la infraestructura tecnológica (hardware, software y comunicaciones), información pública y ciberseguridad y ciberdefensa" (CONPES, 2011: 21).

Como se puede discernir de la estructura con la que cuenta el programa de Ciberseguridad y Ciberdefensa, el objetivo principal que sirve como guía y que rige y ordena estos conceptos y las estrategias adoptadas es alcanzar el fortalecimiento de las capacidades estatales a fin de poder hacerle frente a las amenazas o ataques que potencialmente podrían dañar su seguridad en el escenario cibernético.

En este sentido, el nivel estratégico nacional considera que es primordial que cada agencia de la administración pública se encuentre involucrada dentro de la problemática, y que, por otro lado, cada ciudadano actúe bajo conciencia para instalar en la sociedad en su totalidad la necesidad de que el Estado le garantice estrategias referentes a la seguridad de la información que sean de calidad.

Conclusiones

Como ya se ha dicho precedentemente, el ciberespacio ofrece un gran abanico de oportunidades para desarrollar proyectos de gran utilidad, por lo que muchas veces resulta tentador y eficiente, tanto para individuos como para entidades, ya sea públicas como privadas, debido a las constantes innovaciones y actualizaciones que se hacen en torno a las tecnologías de la información y de las comunicaciones. Sin embargo, este nuevo dominio virtual también acaba siendo foco de amenazas y agresiones hacia ciudadanos comunes y hasta Estados- nación, convirtiéndose en una cuestión referente a la seguridad interior y defensa nacional.

Ante el énfasis que se ha estado depositando sobre este nuevo escenario estratégico en la coyuntura internacional durante esta última década, la UNASUR se vio forzada a comenzar a debatir y a tratar el asunto, ya no desde casos particulares nacionales, sino como un todo, como un organismo regional que, según el Tratado Constitutivo de la Unión de Naciones Suramericanas "busca construir, de manera participativa y consensuada, un espacio de integración y unión en lo cultural, social, económico y político entre sus pueblos […] (2008:02)".

Al respecto, el Consejo de Defensa Suramericano, como órgano regional sectorial encargado de desarrollar tópicos referidos a la defensa de cada uno de los Estados miembros, y por ende, de la defensa a nivel regional, ha comenzado a tomar iniciativas en torno a la adopción, y a la subsiguiente consolidación de estrategias defensivas para evitar ataques contra objetivos vitales en el ciberespacio, logrando grandes avances en la materia. Desde la instalación de la temática en la agenda regional, el

CDS no ha dejado de hacer una labor continua en pos de alcanzar políticas y estrategias en común. Un ejemplo de ello es el foro regional para el intercambio de información, experiencias y procedimientos de solución que se ha establecido, o la red de contactos de autoridades competentes que permite tomar decisiones más significativas en el campo de lo que atañe a la ciberdefensa, y al mismo tiempo, abandonar el carácter esporádico y temporario que adquirían las sesiones de trabajo del grupo de ciberdefensa.

A pesar de ello, continua siendo un obstáculo la diferencia entre los marcos legislativos y doctrinarios que rigen los Sistemas de Defensa Nacional de cada uno de los países miembros de la UNASUR, tornando difícil el esclarecimiento de una tendencia cada vez más fuerte de llegar a una integración total en lo que a defensa, o en particular, a ciberdefensa, se trata. Se ha visto, con los casos estudiados en este artículo que las incompatibilidades entre los tres países desarrollados son grandes debido a la visión que poseen sobre determinados temas. Esto no es casual, sino que deriva de los contextos históricos y de las circunstancias actuales que marcan las políticas públicas que se implementan en las diversas áreas donde actúa el Estado Nacional.

Por otro lado, el Tratado Constitutivo del Consejo de Defensa Suramericano, en su Artículo 3, propone un compendio de principios que la organización deberá considerar al llevar a cabo sus actividades. Uno de ellos hace referencia a la promoción de la reducción de las asimetrías que existen entre los sistemas de defensa de los Estados miembros de la UNASUR, de modo de fortalecer las capacidades de la región en el campo de la defensa (2008), mientras que otro de los principios más relevantes es el "tener presentes los principios de gradualidad y flexibilidad en el desarrollo institucional de la UNASUR y en la promoción de iniciativas de cooperación en el campo de la defensa, reconociendo las diferentes realidades nacionales" (2008).

De ser así, cabe preguntarse, dentro del plano de la ciberdefensa, si es posible avanzar hacia una política, un proyecto en común a nivel regional, respetando las particularidades que presenta cada Estado- nación y consolidando la naturaleza y la esencia de la organización regional.

Como ya se presentó, las diferencias en cuanto a la legislación nacional, a la doctrina, al rol de las Fuerzas Armadas, y a los avances en la estructura concerniente a los organismos responsables de la ciberdefensa y la ciberseguridad son muy grandes, no sólo en las experiencias de los países a los que se refiere el presente artículo, sino. Aún más, la falta de un consenso en torno a conceptos como

ciberdefensa, ciberseguridad, ciberguerra y ciberespacio, y a otros más básicos aún como son la defensa nacional y la seguridad interior, por parte del sector académico y político, dificulta la puesta en escena de una estrategia regional para hacer frente a las posibles amenazas cibernéticas que sufren o potencialmente pueden llegar a sufrir los países de la región.

A pesar de las observaciones hechas, no hay que desdeñar, o subestimar, los objetivos y los avances alcanzados alrededor de este nuevo dominio militar que es el ciberespacio, junto a los fenómenos que lleva consigo, como son la ciberguerra, la ciberseguridad y la ciberdefensa. Si bien, todavía se encuentran vacíos respecto a la terminología y a los conceptos utilizados, al igual que ciertas asimetrías en el desarrollo del tema en los distintos países que conforman la organización regional, es importante mantener en vista el objetivo por el cual se creó la UNASUR y su Consejo de Defensa Suramericano, y así, avanzar, no sólo hacia la consolidación de una estrategia regional de ciberdefensa y al afianzamiento de una identidad suramericana de defensa, sino también, conquistar un espacio participativo y de consenso que unifique a todos los pueblos hermanos de América del Sur.

Bibliografía

DONADIO, Marcela (Coordinadora) (2012), Atlas Comparativo de la Defensa en el Caribe y en América Latina, Buenos Aires, RESDAL, 272 páginas.

DONADIO, Marcela (Coordinadora) (2014), Atlas comparativo de la defensa en América Latina y Caribe, Buenos Aires, RESDAL, 272 páginas. Disponible en: http://www.resdal.org/atlas-2014.html [Consultado el día 12/10/2014]

EISSA, Sergio (2013), "Redefiniendo la defensa: posicionamiento estratégico defensivo regional", Revista SAAP, Buenos Aires, volumen 7, número 1, págs 41-64.

EISSA SERGIO *et al* (2014), "El ciberespacio y sus implicancias para la defensa nacional. Aproximaciones al caso argentino", Revista de Ciencias Sociales, Buenos Aires, número 25, págs. 181-198.

FORTI, Alfredo Waldo (2009), "Centro de Estudios Estratégicos de Defensa: la construcción de una visión estratégica suramericana", Revista de la Defensa Nacional, Ministerio de Defensa de la República Argentina, Buenos Aires, número 5, págs. 68-75.

Ministerio de Defensa de la República Argentina (2009), Consejo de Defensa Suramericano: Una mirada desde la Argentina, Cuadernos de Actualidad en Defensa y Estrategia #4, Buenos Aires, Ministerio de Defensa de la República Argentina.

Documentos oficiales

Unión de Naciones Suramericanas

VII Reunión Ordinaria del Consejo de Jefas y jefes de Estado y de Gobierno de la Unión de Naciones Suramericanas- Declaración de Paramaribo (2013).

Estatuto del Consejo de Defensa Suramericano (2008). Disponible en http://www.ceedcds.org.ar/Espanol/07-Consejo_Defensa_Suramericano/03_Estatuto_CDS.html [Consultado el día 01/10/2014]

V Reunión Ordinaria del Consejo de Defensa Suramericano- I Declaración de Paramaribo.

Plan de Acción 2012 del Consejo de Defensa Suramericano. Disponible en: http://www.ceedcds.org.ar/Espanol/09-Downloads/Esp-PA/Plan-de-Accion-2012.pdf [Consultado el día 03/10/2014]

Plan de Acción 2013 del Consejo de Defensa Suramericano. Disponible en http://www.ceedcds.org.ar/Espanol/09-Downloads/Esp-PA/Plan-de-Accion-2013.pdf [Consultado el día 03/10/2014]

Plan de Acción 2014 del Consejo de Defensa Suramericano. Disponible en http://www.ceedcds.org.ar/Espanol/09-Downloads/Esp-PA/Plan-de-Accion-2014.pdf [Consultado el día 03/10/2014]

Acuerdos bilaterales

Declaración de Buenos Aires de los Ministros de Defensa el Brasil y Argentina (Buenos Aires, 2013)

Declaración Conjunta de los Ministros de Defensa de la República Federativa del Brasil y de la República Argentina (Brasilia, 2013)

Acta de la Reunión del 20 y 21 de noviembre de 2013 del Subgrupo de trabajo bilateral de defensa Cibernética Brasil- Argentina (Brasilia, 2013)

Declaración Conjunta de los Ministros de Defensa de la República Federativa del Brasil y de la República de Chile (Brasilia, 2014). Disponible en http://www.defesanet.com.br/al/noticia/16637/BRASIL-CHILE---Declaracao-Conjunta/ [Consultado el día 13/10/2014]

Argentina

Ley 23. 554 de Defensa Nacional de la República Argentina

Ley 24.059 de Seguridad Interior del a República Argentina

Decreto 727/ 2006 de Reglamentación de la Ley 23.554 de Defensa Nacional.

Decreto 1691/ 2006 de la Directiva de Organización y Funcionamiento de las Fuerzas Armadas

Decreto 1028/ 2003 de disolución de firma digital y creación de la Oficina Nacional de la Tecnología de la Información

Decisión Administrativa 669/ 2004

Disposición ONTI 3/2013

Resolución del Ministerio de Defensa N° 364/ 2006

Resolución del Ministerio de Defensa N° 385/2013

Resolución del Ministerio de Defensa N° 350/2014

Resolución del Ministerio de Defensa N° 351/2014

Brasil

Presidencia de la República Federativa do Brasil (2008), Estrategia de Defensa Nacional, República Federativa do Brasil.

Presidencia de la República. Gabinete de Seguridad Institucional, Secretaria Ejecutiva, Departamento de Seguranca da Informacao e das Comunicacoes (Organizadores: MANDARINO JUNIOR, Raphael; CANONGIA, Cláudia) (2010), Livro Verde – Segurança Cibernética no Brasil. República Federativa del Brasil.

Presidencia de la República Federativa del Brasil. Secretaria de Assuntos estratégicos (2011), Desafíos estratégicos para a Seguranca e Defesa Cibernética, República Federativa del Brasil.

Presidencia de la República Federativa de Brasil, Política de Defensa Nacional (2012). República federativa del Brasil.

Presidencia de la República Federativa del Brasil, Estrategia de Defensa Nacional (2012), República Federativa del Brasil.

Ministerio de Defensa de la República Federativa del Brasil, Livro Branco da Defesa (2012), República Federativa del Brasil.

Ley Complementar N° 136/2010

Ley Complementaria N° 97 sobre las Normas Generales para la Organización, la Preparación y el Empleo de las Fuerzas Armadas.

Colombia

Ministerio de Defensa Nacional de la República de Colombia (2009), Ciberseguridad y Ciberdefensa: Una primera aproximación, República de Colombia

Consejo Nacional de Política Económica y Social (2011), Lineamientos de Política para Ciberseguridad y Ciberdefensa. República de Colombia.

Presidencia de la República de Colombia (2006), Política de Consolidación de la Seguridad Democrática (2006- 2010), República de Colombia.

Presidencia de la República de Colombia (2011), Política Integral de Seguridad y Defensa para la Prosperidad, República de Colombia.

Presidencia de la República de Colombia (2011), Política Nacional de Defensa de la Libertad Personal (2011-2014), República de Colombia.

Ministerio de Defensa Nacional, Ciberseguridad y Ciberdefensa en Colombia (2013), República de Colombia.