LA DEFENSA DE LAS FRONTERAS EN LA AMAZONIA BRASILEÑA Y LA AMENAZA CIBERNÉTICA

En los últimos tiempos se han llevado a cabo profundas modificaciones en el campo estratégico, particularmente en lo referente a la seguridad y defensa. En el siglo XXI, surgieron nuevas manifestaciones de conflictos que atentan contra la seguridad e incluyen a las tecnologías intangibles como la cibernética

PALABRAS CLAVE: **AMENAZA CIBERNÉTICA / GOBERNANZA COLABORATIVA / SISTEMA INTEGRADO DE MONITOREO DE FRONTERAS / AMAZONIA / EJÉRCITO BRASILERO / FRONTERAS**

Por **Paulo Alipio Branco Valença**

INTRODUCCIÓN

Desde hace más de una década se han producido grandes cambios en el escenario estratégico, particularmente en lo referente al entorno y a las condiciones de seguridad y defensa.

En el ambiente estratégico del siglo XXI, Posguerra Fría, y en una coyuntura de orden multipolar, surgieron nuevas manifestaciones de conflictos que atentaban contra la seguridad. Estas son conocidas como nuevas amenazas e incluyen tecnologías intangibles como la cibernética, que puede influir en la protección de la soberanía de un Estado.

Las guerras del mañana no serán como las de ayer, ni las condiciones del entorno estratégico del futuro serán como las de hoy. Sin embargo, el futuro está relativamente próximo y, en consecuencia, es posible determinar los cambios que se exigirán a las Fuerzas Armadas y a la defensa. Así, la dependencia de internet y de sistemas cibernéticos será cada vez mayor para que se pueda lograr un eficiente desplazamiento de fuerzas en un contexto de nuevas dimensiones de tiempo y espacio en el campo de batalla.

Es esencial que las fuerzas armadas del futuro cuenten con un escudo de protección, el cual otorgue seguridad de comunicaciones y garantice el flujo de informaciones en tiempo real, permitiendo, de esta manera, enfrentar al enemigo en el momento y lugar oportuno.

Por la Estrategia Nacional de Defensa, del 2008, y por el Libro Blanco[1] de la Defensa Nacional, del 2012, se constituyeron tres sectores estratégicos fundamentales para la Defensa: el Nuclear, el Cibernético y el Espacial. Como resultado, se asignó al Ejército Brasileño la coordinación del sector cibernético originando la creación del Centro de Defensa Cibernética del Ejército (CDCiber).

Por las dimensiones continentales de Brasil, el tema cibernético gana aún más importancia en un contexto donde la proyección de fuerzas a lugares lejanos constituye un requisito estratégico para el ejercicio pleno de la soberanía, la defensa del territorio y de los espacios aéreos y marítimos.

De este modo, al tema cibernético se le puede agregar la complejidad del territorio brasileño en términos de su geografía, particularmente en la Amazonia que es, según el Libro Blanco de la Defensa Nacional[2]; uno de los focos de mayor interés para la defensa de Brasil y sobre este se afirma su incondicional soberanía.

Este trabajo busca establecer, partiendo de la Política de Defensa Cibernética de Brasil del año 2012, la forma en que el Ejército Brasileño podría combatir las amenazas cibernéticas que puedan afectar el rol de defensa de las fronteras de la Amazonia Brasileña.

En función de esa motivación se buscará contestar a la siguiente pregunta de investigación: La Política de Defensa Cibernética de Brasil, en su concepción, ¿contribuye efectivamente para la defensa de las fronteras en la Amazonia Brasileña?

LAS FRONTERAS AMAZÓNICAS Y LA PRESENCIA DEL EJéRCITO BRASILEñO

Zygmunt Bauman en su libro, La Globalización. Consecuencia humanas, plantea el interrogante *¿Se puede del fin de la geografía, donde las distancias ya no importen y la idea del límite geofísico sea cada vez más difícil de sustentar en el mundo real?*[3]

Probablemente pueda ser así en el futuro pero no en el Brasil de hoy. Las fronteras[4] amazónicas de Brasil[5], aproximadamente de 11.500 km de largo[6], se ubican en áreas aisladas de los grandes centros urbanos y/o con difícil acceso a otras zonas debido a las severas restricciones para los desplazamientos terrestres. Los transportes se realizan casi totalmente por medios fluviales y aéreos. Esta complejidad es potenciada por la porosidad y baja densidad demográfica en un área de 5.016.136,3 km², que corresponde a casi el 59% del territorio brasileño[7].

El Ejército Brasileño se hace presente en la Amazonia desde el siglo XVII y siempre buscó la ampliación del número de sus unidades en esa zona. De ese modo se ha favorecido el surgimiento de polos de desarrollo y núcleos poblacionales que contribuyen al fortalecimiento de la soberanía brasileña.

El Ejército Brasileño se hace presente en la Amazonia desde el siglo XVII y siempre buscó la ampliación del número de sus unidades en esa zona. De ese modo se ha favorecido el surgimiento de polos de desarrollo y núcleos poblacionales que contribuyen al fortalecimiento de la soberanía brasileña.

Más recientemente, el Ejército Brasileño formuló la Estrategia Brazo Fuerte (EBF) considerando las premisas de la Estrategia Nacional de Defensa, del año 2008. En ella se ha considerado que la Amazonia representa uno de los focos de mayor interés para la defensa y deberá tener alta prioridad para la articulación y el equipamiento de las tropas. Bajo esos conceptos fue programado el incremento de la cantidad de unidades en la región de fronteras amazónicas[8].

El Plan de Articulación de la Estrategia Brazo Fuerte incluye el Programa Amazonia Protegida, que reúne un con-

1. El término "Libro Blanco", dentro del ordenamiento gubernamental, es el nombre que se empresta a un documento oficial, publicado por un gobierno o una organización internacional, con la finalidad de exponer una nueva política, u línea de acción sobre un tema actual. Puede servir como fuente de consulta sobre los detalles de una nueva legislación propuesta, en donde haya franco interés gubernamental para su aprobación. Puede, aún, informar o servir de guía sobre algunas de las actividades gubernamentales, presentando como serán gestionados los caminos para la consecución de los objetivos, como por ejemplo: el planeamiento de una política gubernamental de mediano hasta longo plazo. Kitcho, Catherine; *The Launch Pad, October 2004, The Launch Doctor. Rescatado de http://www.pelepubs.com/launchdr/launch_emailnews2.shtml?&id=23LaunchPad Monthly Newsletter - Past Issue.*Traducción del autor.
2. Exército Brasileiro; *Centro de Comunicação Social do Exército;* 2012a.
3. Bauman,Zygmunt; *La Globalización. Consecuencias humanas;* Fondo de Cultura Económica; Buenos Aires; 1999.
4. Hay una aclaración que vale revisar respecto los conceptos geográficos de límite y frontera. El límite es una línea o marco demarcatorio y ya la frontera es algo más amplio, engloba una zona donde pueden desarrollarse relaciones de flujo de bienes capital y personas; Wesley, Maria H. de Amorim; "Fronteiras Transnacionais, Territórios Cibernéticos e os Impactos na Cultura e na Soberania Nacional"; trabajo presentado en el Seminario *Soberanía Nacional y Relaciones Internacionales;* promovido por la ABD; 22 de octubre de 2011; Río de Janeiro; Brasil. Así, la frontera no supone límite preciso entre nacionalidades, etnias, lenguas o religiones; Tello, Antonio; *Diccionario Político.* Voces y locuciones; El Viejo Topo; España; 2012; p. 381.
5. La franja de hasta ciento y cincuenta kilómetros de ancho, a lo largo de las fronteras terrestres, designada como franja de frontera, es considerada fundamental para la defensa del territorio nacional, y su ocupación y utilización serán reguladas en ley (BRASIL, 1988, art. 20o, § 2)". Traducción del autor.
6. Exército Brasileiro; 5ª *Subchefia do Estado-Maior do Exército.* O Exército na Amazônia. Verde Oliva, 2008, pp.12-14.
7. Instituto Brasileiro de Geografia e Estatística - IBGE. (s.f.). Sala de Imprensa IBGE. Rescatado de *http://saladeimprensa.ibge.gov.br/es/noticias?view=noticia&id=1&busca=1&idnoticia =2287*
8. Brasil; Presidência da República; *Livro Branco da Defesa Nacional; Brasília;* DF; 2012a.

junto de proyectos para el fortalecimiento de la presencia militar terrestre en la Amazonia e incluye la creación progresiva de nuevos pelotones especiales de frontera, además de la modernización de los existentes[9].

Simultáneamente, el Ejército prevé la implementación del Sistema Integrado de Monitoreo de Fronteras (SISFRON), el cual comprende la utilización de radares y otros medios electrónicos, interconectando sistemas militares y civiles, con la finalidad de optimizar la capacidad de monitoreo de alrededor de 16.000 km de fronteras de las regiones Amazónica, Centro-Oeste y Sur[10].

El Sistema Integrado de Monitoreo de Fronteras es un sistema integrado de detección para apoyar las decisiones de empleo operativo, cuyo propósito es fortalecer la presencia y la capacidad de acción del Estado en la franja de su frontera. Por medio de este, el Ejército, en cooperación y coordinación con varias agencias, buscará actuar de manera cada vez más eficiente, realizando el monitoreo de las fronteras contra cualquier tipo de amenazas, integrando informaciones provenientes de varios tipos de sensores y de personal presente en el terreno.

Sobre la base del trinomio monitoreo/control, movilidad y presencia, el Sistema Integrado de Monitoreo de Fronteras enfatiza el incremento de Unidades de las Fuerzas Armadas en las fronteras e impulsa la capacitación de la industria nacional brasileña para la conquista de la autonomía en tecnologías indispensables a la defensa.

Más allá de mejorar el control de áreas de la frontera, este Sistema integrado debe asegurar el flujo continuo y seguro de datos entre diversos niveles de la Fuerza Terrestre, produciendo informaciones confiables y oportunas para la toma de decisiones, así como, también, actuando prontamente en acciones de defensa contra fuerzas convencionales o contra delitos trasfronterizos y ambientales, ya sea en operaciones aisladas, conjuntas o interagencias.

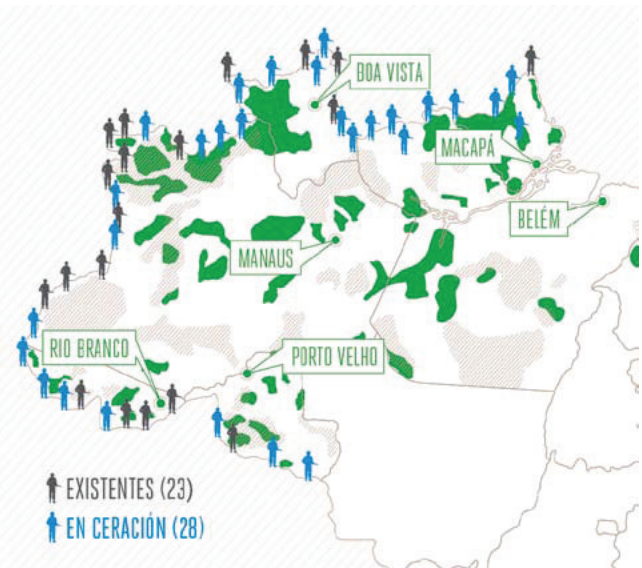
Los medios de detección del Sistema Integrado de Monitoreo de Fronteras estarán desplegados a lo largo de toda la franja de la frontera para potenciar el empleo de las tropas ubicadas en el ámbito de la Amazonía Brasileña.

En síntesis, este Sistema Integrado de Monitoreo es un sistema de sistemas que incluye personas, procesos y estructuras organizacionales, además de una gama integrada de recursos tecnológicos.

Entre los varios componentes del Sistema Integrado de Monitoreo de Fronteras, el Subsistema de Detección[11] empleará radares de vigilancia terrestre y aérea de baja altitud, sensores ópticos, *optrónicos*[12] y sensores de señales electromagnéticas para la recolección de datos para el Subsistema de Apoyo a la Decisión, lo cual aportará al decisor una conciencia situacional, sobre la base de los datos obtenidos.

9. Brasil; Presidência da República; op. cit.
10. Brasil; Presidência da República; op. cit.
11. Con utilización de sensores.
12. Es una nueva rama de la ciencia que surge de la mezcla de la electrónica con la tecnología de las fibras ópticas. Utiliza la alta velocidad de la luz, aliada al hecho de ser posible manipular o trasmitir mensajes luminosas, sin interferencias, por medio de fibras microscópicas, para crear componentes muchísimo menores y más versátiles que sus equivalentes electrónicos. Superinteressante; "Optrônica: A sucessora da eletrônica"; Out 1988. Rescatado de *http://super.abril.com.br/tecnologia/optronica-sucessora-eletronica-438765.shtml*

PELOTONES ESPECIALES DE FRONTERA



Fuente: Exército Brasileiro; Centro de Comunicação Social do Exército; (2012a)

FRANJA DE FRONTERA

Fuente: Exército Brasileiro; Centro de Comunicação Social do Exército; Comando Militar de la Amazonia (CMA); Comando Militar del Oeste (CMO); Comando Militar del Sur (CMS); 2012a

Todo el tráfico de datos se llevará por acción del Subsistema de Tecnología de la Información y Comunicaciones (TIC), el cual tendrá asegurado la confidencialidad, autenticidad, integridad y disponibilidad de las informaciones por el Subsistema de Seguridad de Informaciones y Comunicaciones (SIC) y Defensa Cibernética. El SIC será desarrollado e implementado basado en toda la experiencia existente en el Ejército, a quien le corresponde la coordinación del Sector Cibernético en el ámbito del Ministerio de la Defensa[13].

El Sistema Integrado de Monitoreo de Fronteras apunta a una actuación integrada con instituciones civiles y militares, incluyendo a las de los países vecinos. Su foco es la realización de operaciones interagencias en la franja de frontera.

Correspondiendo con esa labor, el proyecto busca la interacción con sistemas congéneres como el Sistema de Protección de la Amazonía (SIPAM), dependiente del Ministerio de la Defensa, el Sistema de Gerenciamiento de la Amazonia Azul (SisGAAz), a cargo de la Marina de Brasil, y el Sistema de Defensa Aeroespacial Brasileño (SISDABRA), responsabilidad del Comando de la Fuerza Aérea.

Además considera ambientes apropiados para el trabajo interagencias y el establecimiento de enlaces entre los Centros de Operaciones de las Unidades, Brigadas y Comandos Militares del Área con los Gabinetes de Gestión Integrada de Fronteras (GGIF) existentes en los niveles provincial y municipal.

AMENAZAS Y LA POLÍTICA CIBERNéTICA DE DEFENSA DE BRASIL[14]

Las operaciones de defensa de los vastos espacios territoriales de Brasil requieren medios de informática y telecomunicaciones, los cuales pueden sufrir los efectos de las amenazas cibernéticas perpetradas por actores hostiles que utilizan tecnologías informatizadas en el ciberespacio.

Esas acciones suelen provocar la interferencia, violación, daño o destrucción de sistemas, datos o redes de control, comando y comunicaciones. Además, el software malicioso (*malware*), las redes de *Botnets*[15] y las bombas lógicas se pueden emplear para navegar por sistemas de blancos y recuperar datos sensibles[16].

La Guerra Cibernética comprende a las acciones para uso ofensivo y defensivo de informaciones y de sistemas de comunicaciones. Estas acciones permiten la obtención de ventajas tanto en el ámbito militar como en el área de las infraestructuras críticas del Estado y civiles. Esto se logra a través del accionar sobre informaciones, sistemas de informaciones y redes de computadores, con el fin de negar, explorar, corromper o destruir valores del adversario.

14. Instituida por la Decreto Normativo del Ministerio de la Defensa de Brasil No 3.389/MD, de 21 de diciembre 2012.
15. *Botnet* o red de ordenadores zombis es el conjunto formado por ordenadores infectados por un tipo de software malicioso, que permite al atacante controlar dicha red de forma remota. Los equipos que integran la red se denominan "zombis", o también *drones*. Instituto Nacional de Tecnologías de la Comunicación – INTECO; "Botnet ¿Qué es una red de ordenadores zombis?"; *Cuaderno de notas del Observatorio. Rescatado de www.inteco.es/file/p9cSCislwwtRK6aDe7iZKg*
16. Cornish, Paul; Livingstone, David; Clemente, Dave and Yorke, Claire; *On Cyber Warfare.* A Chatham House Report; 2010; p. 49.
17. Wesley, Maria H. de Amorim; op. cit.

El Sistema Integrado de Monitoreo de Fronteras es un sistema integrado de detección para apoyar las decisiones de empleo operativo, cuyo propósito es fortalecer la presencia y la capacidad de acción del Estado Brasilero en la franja de su frontera.

Como lo presenta Wesley[17], el territorio cibernético se vuelve una de las principales amenazas para la Seguridad Nacional debido a que las acciones militares incorporan cada vez más aparatos tecnológicos y, por ende, van quedando cada vez más vulnerables a los ataques cibernéticos o al *ciberterrorismo*.

El Sector Cibernético contempla el empleo de modernos medios tecnológicos enfatizado en las redes de computadores y de comunicaciones destinadas al tráfico de informaciones, ya sean de personas en satisfacción de sus necesidades individuales, o de organizaciones diversas, inclusive aquellas dedicadas a sectores estratégicos del país, como es el caso de la Defensa Nacional.

Este Sector fue introducido en el ámbito de la Fuerza Terrestre por medio del Proyecto Estratégico de Defensa Cibernética, buscando proveer, en forma segura y confiable, la comunicación en red para las Fuerzas Armadas y para toda la nación. En conformidad con lo anterior fue creado el Centro de Defensa Cibernética (CDCiber) para coordinar e integrar los vectores de *ciberdefensa* por medio de *gobernanza*[18] *colaborativa* entre ellos.

Esa política[19] orienta, en el ámbito del Ministerio de la Defensa, a las actividades de Defensa Cibernética en el nivel estratégico y de Guerra Cibernética en los niveles operacional y táctico. Su aplicación alcanza a todos los componentes de la expresión militar del poder nacional y a las entidades que puedan participar en las actividades de Defensa o de Guerra.

En el ámbito del Ministerio de Defensa, las actividades de Defensa Cibernética están orientadas para atender a las necesidades de la Defensa Nacional, teniendo en cuenta que la eficacia de sus acciones depende, fundamentalmente, de la actuación colaborativa de la sociedad brasileña. Esto incluye, también, a la comunidad académica, los sectores públicos y privados y la industria para la defensa.

En consecuencia, las actividades desarrolladas deberán generar libertad de acción asegurando, de forma conjunta, el uso efectivo del espacio cibernético en su preparación y su empleo operacional por parte de las Fuerzas Armadas, impedir o dificultar su utilización contra de los intereses de la Defensa Nacional. También, deberá contribuir a la seguridad cibernética de la información en la Administración Pública Federal y colaborar con la producción de Inteligencia originada en fuentes cibernéticas.

CONCLUSIONES

Puede constatarse en el presente trabajo la complejidad de las fronteras terrestres de Brasil y las codicias por sus riquezas amazónicas. Para contrarrestar estos riesgos estratégicos, el Ejército Brasileño tiene desplegadas varias unidades militares en la zona y sigue aumentando la cantidad de tropas en la región, lo que se denomina Estrategia de la Presencia. Además, se ha buscado utilizar recursos tecnológicos informatizados para el monitoreo y control de la frontera por medio del Sistema Integrado de Monitoreo de Fronteras, el cual se enlaza con otros sistemas defensivos de las demás fuerzas armadas.

Paralelamente, al Ejército Brasileño le están asignados los roles de ejercer la *gobernanza colaborativa,* la coordinación e integración de los vectores de *ciberdefensa* del país, por medio del Centro de Defensa Cibernética (CDCiber). De ese modo se ha otorgado al Ejército Brasileño la capacidad institucional propia de garantizar la eficiencia del Sistema Integrado de Monitoreo de Fronteras y, consecuentemente, generar libertad de acción para las operaciones de sus unidades con presencia en la Amazonia.

Puede verificarse también que la Política de Defensa Cibernética de Brasil, por su alcance, objetivos y directrices, ampara totalmente los sistemas de vigilancia, seguridad y defensa de las fuerzas armadas y de otras instituciones en sus roles de defensa de las fronteras amazónicas.

Por lo tanto, existe total coherencia en la estrategia de fines y medios integrados para que el Ejército Brasileño pueda combatir las amenazas cibernéticas a través del Sistema Integrado de Monitoreo de Fronteras, apoyándose en el Centro de Defensa Cibernética del Ejército y manteniéndose en línea con los postulados de la Política de Defensa Cibernética de Brasil.

Paulo Alipio Branco Valença
Coronel del Ejército de la República Federativa de Brasil. Oficial de Estado Mayor. Egresó, en el 2013, de la Escuela Superior de Guerra Conjunta del Curso de Estrategia y Conducción Superior.

18 Gobernanza: Modo de gobernar o habilidad para hacerlo orientado a la obtención de un desarrollo económico, social e institucional sostenible basándose en una relación equilibrada entre el Estado, la sociedad civil y el mercado. Tello, Antonio; op. cit.

19. Ministério da Defesa da Brasil; *Política Cibernética de Defesa;* Portaria normativa no- 3.389/md; de 21 de dezembro DE 2012. Brasília, DF, 21 dezembro 2012; *Política Cibernética de Defesa;* Portaria normativa No- 3.389/MD; de 21 de dezembro de 2012; Brasília; DF; 21 dezembro 2012.