LA AMENAZA CIBERNÉTICA PARA LA SEGURIDAD Y DEFENSA DE BRASIL

En el siglo de la Revolución Digital, la tecnología se ha vuelto un factor de vital importancia. Sin embargo, internet puede tornarse un arma de doble filo, presentándose en ocasiones como una herramienta útil y, en otras, como una amenaza que debe mantener siempre alerta a las instituciones que controlan la seguridad y defensa de un estado. Es por esto que Brasil ha optado por tomar medidas para hacer frente a una latente amenaza cibernética

PALABRAS CLAVE: **CIBERGUERRA / AMENAZA / SEGURIDAD / VULNERABILIDADES**

Por **Augusto Cesar Amaral**

El siglo XXI es llamado el de la Revolución Digital debido al avance en informática y telecomunicaciones. Como toda herramienta, la tecnología puede ser usada para el progreso de la humanidad o para cualquier otro propósito. Hoy no puede decirse que un país, cualquiera que sea, esté libre de sufrir un ataque cibernético que signifique no solo delito cibernético sino, también, una agresión cibernética estatal en sus diferentes formas.

Así, la amenaza cibernética afecta la seguridad y defensa de cualquier estado. Brasil no es la excepción. Sin embargo, ¿cuál es la magnitud de esta amenaza? ¿Cuáles son los principales factores de vulnerabilidad?

Tomando como punto de partida la Política Nacional de Defensa de Brasil, publicada en el 2005, se va a plantear la forma en la cual se están estructurando sus capacidades para la Seguridad y Defensa Cibernética de la Infraestructura Crítica Nacional y responder: ¿Es Brasil capaz de proveer una defensa efectiva contra los ataques originados en un escenario cibernético cada vez más hostil?

CONCEPTOS Y DEFINICIONES

El gran salto tecnológico que se ha producido en los últimos 30 años en el campo de las Tecnologías de la Información y las Comunicaciones (TIC) ha provocado cambios significativos en la forma en que los individuos, las organizaciones y las naciones se relacionan y se estructuran.

Hoy en día, se percibe un alto grado de dependencia de los individuos, grupos sociales, organizaciones públicas y privadas, las estructuras críticas para la gobernabilidad, la seguridad y la defensa de un país, con los sistemas informáticos interconectados por medio de complejas redes de procesamiento de datos. Estos son vulnerables a ataques y fraudes

perpetrados por diversos agentes, en un nuevo espacio de interacción denominado ciberespacio:

Un ámbito caracterizado por el uso de la electrónica y el espectro electromagnético para almacenar, modificar e intercambiar datos a través de los sistemas en red y la infraestructura física asociada. El ciberespacio se puede considerar como la interconexión de los seres humanos a través de los ordenadores y las telecomunicaciones, sin tener en cuenta la dimensión física[1].

...incluye la arquitectura organizadora de la Internet, los dispositivos conectados a la Internet y las redes convencionales e inalámbricas. Algunas de esas redes son administradas por entidades del gobierno y del sector privado, algunas están conectadas a la Internet más amplia y algunas no[2].

En esencia, seguridad significa condición de seguro, libre de riesgos y/o amenazas, peligros, daños y en el caso de existir, estar en condiciones de defenderse con altas probabilidades de éxito. Por su parte, defensa es la/s acción/es llevada/s a cabo para protegerse de tales riesgos, amenazas, peligros y daños[3].

Así se puede decir que, en el ámbito de un estado, la seguridad cibernética se refiere a la protección y garantía de uso de los activos estratégicos de información que controlan la infraestructura crítica nacional[4]. La defensa cibernética es el establecimiento de acciones defensivas y ofensivas, en el contexto de una planificación militar, efectuadas en el ciberespacio, que pueden generar la guerra cibernética.

LAS AMENAZAS CIBERNÉTICAS Y LAS VULNERABILIDADES

Numerosas son las noticias de ataques cibernéticos a los ciudadanos, organizaciones, empresas y estructuras críticas de un país. Pueden venir de cualquier parte, es muy difícil identificar a su autor o fuente. Pueden ser cometidos por jóvenes aficionados sin grandes intenciones, grupos criminales de fraude económico, empresas de espionaje industrial, grupos terroristas para fines políticos e incluso por agentes estatales.

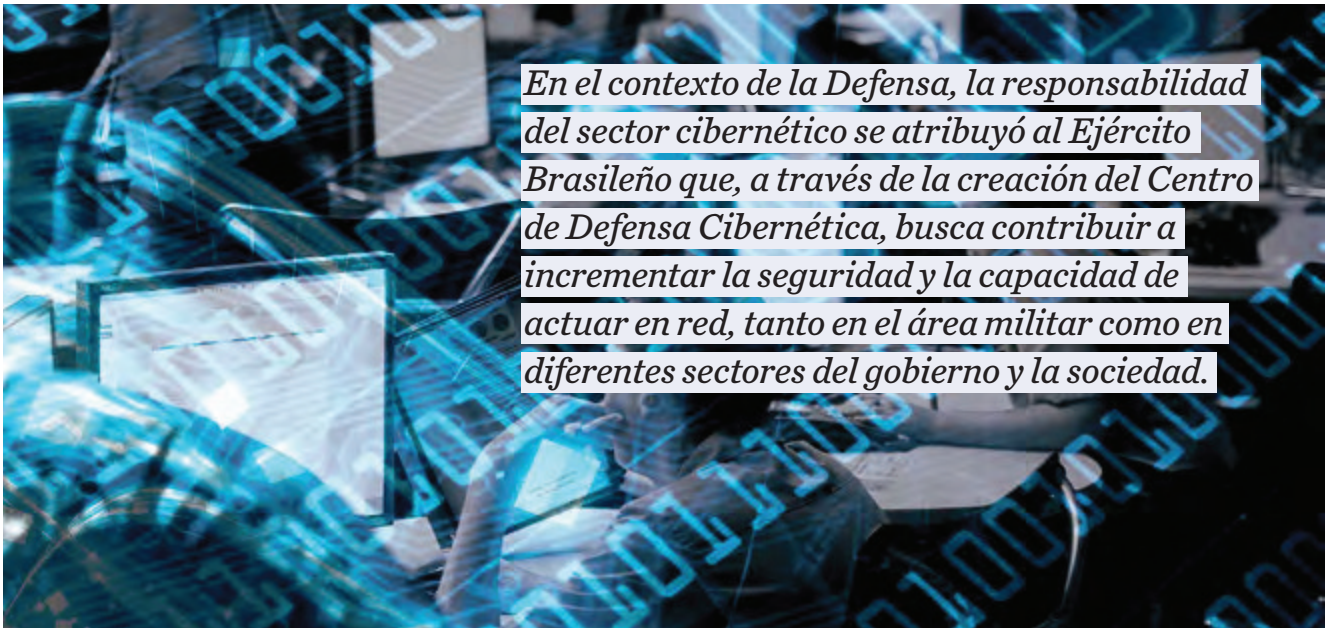
Las vulnerabilidades de los sistemas y los riesgos asociados son numerosos. La mayoría de los actos cometidos provienen de la atracción que el ciberespacio produce al ofrecer una mayor rentabilidad, globalidad, facilidad e impunidad para todo tipo de actividades.

Los conflictos pueden ser tan simples como disputas civiles sobre la propiedad de un nombre de dominio o, más complejos, como campañas deliberadas de ataques cibernéticos como parte de la guerra convencional entre estados avanzados tecnológicamente.

Es importante distinguir la diferencia entre delitos y amenazas cibernéticas, debido a que la mayoría de los delitos cibernéticos ni siquiera constituyen una amenaza para la seguridad del país al no afectar a su infraestructura crítica, debiendo ser tratados en el ámbito de la justicia y el derecho.

Sin embargo, algunos analistas consideran que: la sensación de inseguridad en la red y de la alarmante existencia de cibercrímenes no es sino producto de recursos de información creados artificialmente por la propia industria de ciberseguridad que, sin duda, tiene interés en la dramatización de los cibercrímenes; esto es, en la creación de una sensación subjetiva de inseguridad y alarma en la red[5].

Otros, como David Betz y Thomas Rid cuestionan el uso del término ciberguerra, diciendo:



La amenaza cibernética afecta la seguridad y defensa de cualquier estado. Brasil no es la excepción. Sin embargo, ¿cuál es la magnitud de esta amenaza? ¿Cuáles son los principales factores de vulnerabilidad?

La palabra ciberguerra es sugerente, sin duda, pero ¿qué significa realmente para los estrategas preocupados por el equilibrio de los fines, los medios en los conflictos hoy en día? No mucho. De hecho, no es sólo un neologismo de sentido, pero estratégicamente una distracción y sin sentido alguno. Estrategas contemporáneos que consideran que ciberguerra es una nueva forma decisiva del conflicto se equivocan[6].

La Ciberguerra nunca sucedió en el pasado: esto no ocurre en el presente, y es muy poco probable que moleste a nuestro futuro. Todos los anteriores y actuales ataques cibernéticos políticos - en contraste con los delitos informáticos - son versiones sofisticadas de tres actividades que son tan antiguas como el propio conflicto humano: el sabotaje, el espionaje y la subversión[7].

EN BRASIL

En el 2005, después de un largo período de tiempo sin una política de defensa, el Gobierno Brasileño emitió su Política de Defensa Nacional – PND[8], documento que tiene el objetivo de concientizar a todos los sectores de la sociedad brasileña sobre la importancia de la defensa del país.

Establece que el sector cibernético es estratégico para la Defensa Nacional, que debe fortalecerse para minimizar la vulnerabilidad de los sistemas que tienen soporte para tecnología de la información y la comunicación, o permitir su pronta recuperación. Por lo tanto, debe ser capaz de oponerse a los posibles ataques cibernéticos.

A su vez, la Estrategia Nacional de Defensa – END (2008), cuando se trata de seguridad nacional y de las medidas para la seguridad de las infraestructuras críticas, impone *el perfeccionamiento de los dispositivos y procedimientos de seguridad que reduzcan la vulnerabilidad de los sistemas relacionados a la Defensa Nacional contra ataques cibernéticos y, si fuere el caso, que permitan su pronto restablecimiento, a cargo de la Casa Civil de la Presidencia de la República, de los Ministerios de Defensa, de Comunicaciones y de Ciencia y Tecnología, y del Gabinete de Seguridad Institucional de la Presidencia de la República (GSI/PR).*

El Gabinete de Seguridad Institucional, órgano coordinador de la actividad de la seguridad de información en Brasil lanzó, en el 2010, el *Libro Verde de Seguridad Cibernética* con el fin de crear las condiciones necesarias de seguridad cibernética, con respecto a la comprensión de los nuevos requerimientos para la protección de la sociedad y el Estado Brasileño.

Este libro procura afrontar el desafío de conciliar las agendas del gobierno, de las academias, del sector privado y del tercer sector[9], a un esfuerzo participativo para construir un pensamiento común y las directrices de una Política Nacional de Seguridad Cibernética, abarcando los siguientes vectores: el político-estratégico, el económico, el social y ambiental, comunicaciones y tecnología de la información, la educación, el legal, la cooperación internacional y la seguridad de las infraestructuras críticas. Percibe a la seguridad cibernética como una función estratégica del estado y esencial para el mantenimiento y la preservación de las infraestructuras críticas del país, tales como energía, transporte, telecomunicaciones, agua, finanzas, información, entre otros.

La responsabilidad del sector cibernético, en el contexto de la Defensa, se atribuyó al Ejército Brasileño que, a través de la creación del Centro de Defensa Cibernética, busca con-

1. Bejarano, María José Caro; "Alcance y Ámbito de la Seguridad Nacional en el Ciberespacio"; *Cuadernos de Estrategia 149; Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio;* Instituto Español de Estudios Estratégicos; Ministerio de Defensa de España; 2011; capítulo 1; pp. 49 – 82. Rescatado de *http://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf*
2. Chang, W., & Granger, S.; "La Guerra en el Ámbito Cibernético"; *Air & Space Journal* - español, volumen 24, Nro, 3; pp. 83 - 90. Rescatado de *http://www.airpower.au.af.mil/apjinternational/apj-s/2012/2012-3/2012_3_10_chang_s.pdf*
3. de Vergara, Evergisto; "Las diferencias conceptuales entre Seguridad y Defensa"; Instituto de Estudios Estrategicos de Buenos Aires – IEEBA; febrero de 2009. Rescatado de http://*www.ieeba.com.ar/colaboraciones2/Las%20diferencias.pdf*
4. Infraestructuras Críticas son las instalaciones, servicios, bienes y sistemas cuya interrupción o destrucción, en todo o en parte, causará grave impacto social, económico, político, ambiental, internacional o de seguridad del Estado y la sociedad; Brasil; Gabinete de Segurança Institucional; *Livro Verde: segurança cibernética no Brasil;* 2010.
5. González Cussac, José Luis; "Estrategias legales frente a las ciberamenazas"; *Cuardenos de Estrategia;* Nro. 149; *Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio* Instituto Español de Estudios Estratégicos; Ministerio de Defensa de España; 2011; capítulo II; pp. 85 - 127. Rescatado de *http://www.cni.es/comun/recursos/descargas/Cuaderno_IEEE_149_Ciberseguridad.pdf*
6. Betz, D.; "Cyber war is not coming. Infinity Journal"; Issue Nro. 3, Summer; 2001; pp. 21 – 24. Rescatado de *https://www.infinityjournal.com/article/23/Cyberwar_is_not_coming/*
7. Rid, T.; *The cyber war will not take place.* London: C. Hurst & Co.Ltd; 2013.
8. Decreto Nº 5484; del 30 de junio de 2005; Brasil. Rescatado de *http://www.planalto.gov.br/ccivil_03/_Ato2004-2006/2005/Decreto/D5484.htm*
9. Suele llamarse Tercer Sector a un conjunto de instituciones cuya característica principal es ser "privadas pero no lucrativas" y desenvolverse en el espacio público para satisfacer demandas no satisfechas ni por el Estado, ni por el Mercado. Se trata de un espectro altamente diverso de organizaciones que actúa dentro del sector no lucrativo (Organizaciones no Gubernamentales, Fundaciones, Comedores Escolares, Cooperativas, etcétera), a la que los autores suelen denominar de diferentes modos, tales como: Sector No Lucrativo o Sin Fines de lucro, Economía Social o Solidaria, Tercera Vía o Tercer Sector.
10. Portaria Normativa; Nº 3389 /MD; Brasil; de 21 de diciembre de 2012. Rescatado de *https://www.defesa.gov.br/arquivos/File/legislacao/emcfa/publicacoes/md31_p_02_politica_cibernetica_de_defesa.pdf*

La defensa cibernética es el establecimiento de acciones defensivas y ofensivas, en el contexto de una planificación militar, efectuadas en el ciberespacio, que pueden generar la guerra cibernética.

tribuir a incrementar la seguridad y la capacidad de actuar en red, tanto en el área militar como en diferentes sectores del gobierno y la sociedad.

El Centro de Defensa focaliza sus acciones en la formación de recursos humanos, la actualización doctrinaria, el fortalecimiento de la seguridad, la respuesta a incidentes en la red, la incorporación de las lecciones aprendidas y la protección contra los ataques cibernéticos.

Continuando con el proceso en curso, el Ministerio de Defensa publicó, en el 2012, un documento que detalla la Política de Defensa Cibernética[10] y establece las directrices del Sistema Militar de Defensa Cibernética (SMDC) para consolidarse. El documento indica las tareas de las Fuerzas Armadas en la prevención del uso criminal de internet y otras redes, así como la protección de los datos y las comunicaciones esenciales.

SISTEMA DE SEGURIDAD Y DEFENSA CIBERNÉTICA

Hoy en día se puede decir que Brasil está a un paso de consolidar el Sistema de Seguridad y Defensa Cibernética Brasileño. Éste tendrá alcance nacional, emanando desde el más alto nivel político, representado por el Gabinete de Seguridad Institucional (GSI/PR) y la Administración Pública Federal (APF), pasando por el Ministerio de Defensa (MD), que realiza el enlace político-estratégico, llegando hasta los niveles más bajos de mando de las Fuerzas Armadas, que actúan a nivel operacional y táctico, con el fin de involucrar a toda la sociedad en la defensa de los intereses nacionales en el ciberespacio.

En este sistema, el Gabinete de Seguridad (GSI/PR) coordina las acciones que afectan a la seguridad de la sociedad y del Estado: Seguridad Cibernética, Seguridad de la Información y Comunicaciones (SIC) y la Seguridad de las Infraestructuras Críticas Nacionales.

Además de contribuir al esfuerzo nacional en las áreas de seguridad, el Ministerio de Defensa está a cargo de las operaciones de características de Defensa Cibernética.

Para ello, las Fuerzas Armadas han recibido la siguiente orden:

- **A nivel estratégico:** llevar a cabo las acciones necesarias para su desempeño en situaciones de crisis o de conflicto armado y con carácter episódico en una situación de paz y normalidad institucional.
- **A nivel operativo:** ejecutar las acciones defensivas y ofensivas, relativas a la preparación y el empleo en las operaciones militares de cualquier naturaleza e intensidad que caracterizan el ambiente de guerra cibernética.

CONCLUSIONES

¿Es capaz Brasil de proveer una defensa efectiva contra los ataques originados en un escenario cibernético cada vez más hostil?

Hoy en día, se puede afirmar que ningún país es capaz de defenderse contra ataques cibernéticos con plena efectividad. El entorno es muy cambiante y a cada momento surgen nuevas amenazas. Los sistemas de información y procesamiento de datos, en general, son muy vulnerables y, los actores implicados, muy distintos entre sí.

Resulta imposible predecir un ataque o identificar su origen con exactitud. Los sectores de seguridad centran sus acciones en la identificación y eliminación de los puntos de vulnerabilidad de los sistemas empleados y en la capacidad de recuperarse y no replicación de los daños posataque.

En este sentido, Brasil, al igual que otros países, tiene como objetivo desarrollar la conciencia e involucrar los diversos sectores de la sociedad brasileña, incluidas la clase política, las fuerzas armadas, la academia, el sector privado y el tercer sector, en el problema de la seguridad y defensa cibernética.

Brasil ha trabajado para organizar y capacitar a los órganos de: la seguridad y defensa cibernética; la seguridad de la información y de las comunicaciones y la seguridad de las infraestructuras críticas, los cuales desarrollan actividades que se complementan y se superponen.

Ha diseñado, a su vez, el Sistema de Seguridad y Defensa Cibernética Brasileño, el cual es coordinado por el Gabinete de Seguridad Institucional de la Presidencia de la República en acciones de seguridad y cuenta con el apoyo del Ministerio de Defensa en lo relativo a las acciones de defensa.

Allí, la defensa cibernética tiene como principal vector el Centro de Defensa Cibernética de Brasil, unidad militar recientemente creada con el objetivo de generar conocimiento y doctrina, capacitar recursos humanos y aplicar las medidas defensivas y ofensivas de la guerra cibernética.

Se concluye entonces que Brasil reúne todas las condiciones necesarias para desarrollar su Sistema de Seguridad y Defensa Cibernética y, así, poder hacer frente a cualquier ataque que pueda afectar el funcionamiento de sus infraestructuras críticas.

› ARTÍCULO CON REFERATO

Augusto Cesar Amaral
Coronel de la Fuerza Aérea de la República Federativa de Brasil. Oficial de Estado Mayor. Egresó de la Escuela Superior de Guerra Conjunta en 2013, del Curso de Estrategia y Conducción Superior.