ARTÍCULO DOI 10.22491/cmm.a003

Un análisis sobre el proceso de titulización del ciberespacio*

An analysis of the cyberspace securitization process

Resumen: El ciberespacio se manifiesta como nuevo dominio para las relaciones de poder en la medida que distintos actores lo utilizan para perseguir sus intereses. Por ser dotado de una lógica de desterritorialización (pérdida de territorio) – en la cual múltiples órganos pueden actuar de manera anónima –, el ciberespacio desafía concepciones tradicionales de seguridad y defensa nacional, mientras que flujos digitales cruzan distintos territorios. Es considerada la inserción de la infraestructura básica de un Estado en el dominio cibernético, englobando sistemas bancarios, de telecomunicaciones, transportes y diversos agentes, como los militares, se observa una creciente dependencia de la sociedad con respecto al ciberespacio. Tal dependencia puede ser explotada por una miríada de actores internacionales. En ese contexto, por intermedio de la concepción de la Escuela de Copenhague con respecto del proceso de reconocimiento de amenazas por agentes de titulización, el presente artículo investiga el proceso de titulización del ciberespacio mediante análisis de los libros blancos de defensa de Brasil, Alemania y Francia.

Palabras Clave: Ciberespacio. Seguridad. Defensa. Territorio. Amenazas.

Abstract: Cyberspace manifests itself as a new domain for power relations as different actors use it to pursue their interests. Because it is endowed with a deterritorializing logic - in which multiple entities can act anonymously - cyberspace defies traditional conceptions of national security and defense, as digital flows cross different territories. Considering the insertion of the basic state infrastructure in the cyber domain, encompassing banking, telecommunications, transport and military systems, there is a growing dependence of society on cyberspace. Such dependency can be exploited by a myriad of international actors. In this context, through the conception of the Copenhagen School regarding the process of recognition of threats by securitizing agents, this article investigates the process of securitization of cyberspace by analyzing the white defense books of Brazil, Germany and France.

Keywords: Cyberspace. Safety. Defense. Territory. Threats.

Breno Pauli Medeiros
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
breno.pauli@gmail.com

Alessandra Cordeiro Carvalho
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
alessandraccarvalho27@hotmail.com

Luiz Rogério Franco Goldoni
Exército Brasileiro, Escola de Comando e Estado-Maior do Exército, Instituto Meira Mattos.
Rio de Janeiro, RJ, Brasil.
luizrfgoldoni@gmail.com

Recibido: 13 dic. 2018
Aceptado: 24 ene. 2019

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

* Ese artículo forma parte de los esfuerzos de investigación del proyecto 'Ciencia, Tecnología e Innovación en Defensa: Cibernética y Defensa Nacional', fue aprobado por el Pliegue de Condiciones 27/2018, Programa de Apoyo a la Enseñanza y a la Investigación Científica y Tecnológica en defensa Nacional – PRO-DEFENSA IV

1 Introducción

El espacio cibernético representa un nuevo dominio de las relaciones de poder. Dada la naturaleza desasociada, en parte, del espacio físico, el ciberespacio se presenta con lógica propia, en la cual la concepción tradicional de fronteras difícilmente impide el flujo de informaciones en el dominio cibernético. Como nuevo ambiente operativo, el ciberespacio integra acciones privadas, militares, civiles y estatales al medio técnico-científico-informacional. Mientras que el espacio cibernético se consagra como un dominio alternativo para el ejercicio de las relaciones de poder, sus lógicas y peculiaridades engendran retos a los dominios tradicionales.

En consecuencia de la disminución de distancias físicas, instantaneidad de las comunicaciones y mayor interdependencia de la sociedad para con el ciberespacio, surgen cuestionamientos sobre como pensar la defensa y la estrategia en ese nuevo dominio. De entre esos, se destacan indagaciones sobre titulización y cuáles serían las "nuevas" amenazas.

En ese nuevo ambiente – marcado por la flexibilización de fronteras y territorios, multiplicidad y anonimato de actores – nuevas y antiguas amenazas desafían las concepciones tradicionales de seguridad y defensa nacional. Es notable la frecuencia de hechos cibernéticos en el escenario internacional. Ataques por *malwares*[1], *ransomwares*[2], DDoS[3], entre otros, además de expandir el número de posibles agresores para actores no necesariamente estatales, está convirtiéndose todavía más sofisticados, dificultando la identificación de la autoría o motivaciones para los ataques. Delante de ese escenario de inseguridad, el ciberespacio puede ser interpretado como un dominio para el ejercicio de poder, en paralelo con los dominios terrestre, marítimo, aéreo y espacial.

La presente investigación tiene como objetivo investigar el proceso de titulización del ciberespacio en Brasil, Alemania y Francia, desde el análisis de contenido comparado entre sus respectivos Libros Blancos de Defensa. Estudiar los documentos de defensa de los países seleccionados posibilita evidenciar las amenazas, las estrategias y las prácticas que compone el proceso de titulización del ciberespacio en Estados que fueron objetivos de espionaje y monitoreo en el espacio cibernético (BRIDI; GREENWALD, 2013; WIKILEAKS, 2015).

Dadas las limitaciones del presente trabajo, serán analizados el *White Paper on German Security Policy and The Future of the Bundeswehr*, el *French White Paper: Defense and National Security* y el Libro Blanco de defensa Nacional de Brasil, seguido de su versión más reciente, la minuta de 2016. El análisis fue limitado a los Libros Blancos de defensa de los países, una vez que esos representan los documentos de defensa de más alto escalón, determinando el tono y el abordaje de los documentos que los siguen jerárquicamente.

Con el objetivo de direccionar el análisis de contenido de esos documentos, la investigación será constituida por cuatro preguntas principales: i) ¿Existe alguna definición clara de seguridad

1 Los tipos más comunes de *malwares o "malicious software"* son los virus o *worms* (vermes), los cuales poseen la capacidad de ocasionar daños y auto replicarse en redes de ordenadores y sistemas (GOLDANI, 2005).

2 Tipo de *malware* rentable que permite la inaccesibilidad de datos almacenados en ordenadores, una vez que los transforma en datos encriptados, exigiendo del usuario pagos de rescate (SYMANTEC, 2016).

3 Técnica de ataque que involucra una gran cuantidad de ordenadores – pudiendo ser de conocimiento del propietario o no –, que sobrecarga sitios o servidores por medio de la saturación de solicitudes de servicios, generando la indisponibilidad del sistema (CARREIRO, 2012).

cibernética en los documentos?; ii) ¿El que los documentos exprimen sobre el sector cibernético?; iii) ¿Cuáles son las amenazas consideradas? y iv) ¿Cuál es el posicionamiento en relación al involucramiento de otros sectores de la sociedad? En paralelo, será realizado un análisis comparativo de los libros blancos de defensa en los aspectos que abordan las nuevas y tradicionales amenazas correlacionadas a cuestión cibernética, además de términos clave que contribuyen para la comprensión con respecto a la relevancia de los asuntos que fueron propuestos, mediante la elaboración de tabla comparativas y aglomeraciones de palabras que exprimen el tono y los términos más prominentes en cada documento.

De acuerdo con la sociedad actual se inserta en el ciberespacio, actores lo utilizan para la proyección de fuerza e intereses. El carácter desterritorializador inherente al dominio cibernético permite, por ejemplo, que grupos terroristas recluten disidentes; agencias de inteligencia monitoreen comunicaciones, y activistas de movimientos sociales coordinen sus manifestaciones.

Esencialmente, el espacio cibernético surge como un espacio alternativo y paralelo a los dominios tradicionales de tierra, aire y mar; sin embargo, el ciberespacio no posee fronteras, espacio aéreo y ni aguas nacionales (HILDEBRANDT, 2013). Para que un actor opere en el ciberespacio, no es necesaria una unidad de blindados, cacerías o navíos, basta una conexión con el Internet. De esa manera, la difusión de poder inherente al ciberespacio proporciona un dominio operativo para actores particulares en paralelo con fuerzas estatales (NYE, 2012). Factor que, simultáneamente, dota el ciberespacio de valor estratégico para los Estados, y puede representar un nuevo ambiente del cual emanan amenazas no necesariamente estatales.

Considerada la creciente pertinencia de la cibernética en el contexto de seguridad y defensa, el presente trabajo se justifica desde el momento que representa un esfuerzo analítico con respecto del proceso de titulización del ciberespacio como dominio estratégico por potencias regionales. No obstante, antes de analizarse tal proceso en Brasil, Alemania y Francia, se hace necesario presentar algunos conceptos y definiciones para una mejor contextualización sobre el tema.

2 **El ciberespacio: contextualización, conceptos y definiciones**

El espacio cibernético posee diversas definiciones – algunas de más alcance de que otras –, que contribuyen para la existencia de un amplio espectro de abordajes y comprensiones (KUEHL, 2009). Algunas consideran en el aspecto más teórico, como una nueva área de interacción que alcanza e interconecta las telecomunicaciones en una gran red global, otras consideran los aspectos físicos y maleables de las distintas conexiones y dispositivos interconectados.

Lobato y Kenkel (2015, p. 24-25, nuestra traducción) comprenden el ciberespacio de manera amplia, como "la red de informaciones mundial interconectada y la infraestructura de comunicaciones que engloba el Internet, redes de telecomunicaciones, sistemas de ordenadores y las informaciones contenidas en ellos". La definición propuesta por los autores, propone un abordaje amplio del concepto de espacio cibernético como siendo una gran red de comunicaciones interconectadas que engloba diversos actores conectados a ella.

Libicki (2009) ofrece una definición más específica, pues interpreta el espacio cibernético como un medio menos tangible que los tradicionales dominios de tierra, aire y mar. Para el autor, el espacio cibernético es compuesto por tres camadas interconectadas: la primera es representada por el *hardware*, componentes electrónicos físicos, en la forma de hilos, antenas, y toda suerte de

dispositivos interconectados, incluyendo desde ordenadores y teléfonos móviles a los sistemas de armamentos, vehículos aéreos no tripulados (VANT), y así por delante. La segunda camada – o sintáctica –, consiste en el *software*. En esa se encuentran las instrucciones y los comandos que los desarrolladores e ingenieros dan a los elementos de la primera camada para que los mismos cumplan su objetivo y se comuniquen unos con los otros. Por último, está la camada semántica, en la cual las informaciones son contenidas en la forma de datos binarios a ser organizados en líneas de código o cualquier otro tipo de información.

En ese contexto, el ciberespacio puede ser entendido como un dominio existente mediante la interconectividad de flujos informacionales, en el cual se inserten todos los tipos de redes e infraestructuras críticas para la sociedad hodierna. Luego, desde el momento que hay conexión entre uno o más dispositivos, el espacio cibernético se convierte realidad, sirviendo como una plataforma para variadas relaciones humanas. Por alcanzar actores distintos, el ciberespacio es escenario para novedosas relaciones de poder. Estas engendran distintas amenazas que interaccionan, modifican y exploran los flujos informacionales del dominio cibernético.

El análisis del ciberespacio demanda especial atención a tres elementos esenciales. Estos representan peculiaridades inherentes al ciberespacio e imponen retos teóricos y prácticos a las relaciones sociales. El primer elemento es la desterritorialidad del espacio cibernético. Considerando los elementos físicos de la camada de *hardware* como dispositivos que actúan de manera análoga a nudos en una gran red de comunicaciones globales, compuesta por flujos de informaciones, se comprende que esos flujos informacionales corresponden a una lógica reticular inherente exclusivamente al espacio cibernético que interconecta los distintos dispositivos físicos interconectados por el ciberespacio. Se subraya que las tradicionales definiciones e interpretaciones de territorio el comprenden como el área geográfica delimitada por fronteras, correspondiendo a la una lógica zonal mediante el recorte espacial, en la cual el Estado realiza el control soberano del territorio[4].

La desterritorialidad del ciberespacio se hace presente desde el momento que su lógica reticular, en la forma de flujos interconectados, alcanza el territorio de distintos Estados; o cuando los dispositivos que sirven de nudos en la red del ciberespacio son controlados y/o son explotados por otros Estados. O sea, la interconectividad de distintos puntos en una red global termina por alcanzar[5] las fronteras, son tenidas como fundamentales para la lógica zonal en la cual el concepto de territorio es fundamentado.

El segundo elemento corresponde a la difusión de poder en el espacio cibernético. De acuerdo con el dominio cibernético surge como espacio alternativo para el ejercicio del poder, la multiplicidad de actores en la red, en conjunto con la facilidad del acceso y adquisición de equipos y capacidades permiten la relativa reducción del alejamiento de capacidades entre Estados militarmente más fuertes, Estados fragilizados, organizaciones y/o individuos no estatales. En ese contexto, el número de amenazas en potencial crece exponencialmente, una vez que nuevos actores utilizan el espacio cibernético tanto para el ejercicio de *soft* cuanto de *hard power* (NYE, 2012). De

4 La concepción de lógica reticular y zonal parte del análisis de territorio-red, idealizada por Haesbaert (2007), en la cual las distintas territorialidades de grupos e individuos se mezclan con la hegemonía territorial de Estados. El abordaje que, aquí, fue utilizado, sin embargo, usa el término en el sentido más específico al ciberespacio, considerado la lógica reticular de los flujos informacionales dentro de la red del ciberespacio que alcanza las fronteras de la concepción zonal de los territorios estatales.

5 Se trata de una generalización. Es sabido que países como China y Corea del Norte poseen amplias restricciones al uso de sus telecomunicaciones y acceso a la red global de ordenadores.

hecho, Marcos Guedes de Oliveira (2014), al tratar del potencial inexplorado de la guerra cibernética, alerta para las eventuales consecuencias resultantes de la actuación de individuos en el ciberespacio que pueden venir a afectar sistemas de los cuales la sociedad depende. Segundo el autor:

> Un nuevísimo campo de acción está relacionado con la facilitación de insurrecciones, manifestaciones y mismo golpes vía uso y manipulación de recursos compartidos por las redes de telefonía celular. El éxito en operaciones con ese formato reduciría en mucho los costos de intervención abierta y militar en países menores y daría a las naciones dominantes de esa tecnología un fuerte argumento en favor de la no reglamentación internacional del medio cibernético (OLIVEIRA, 2014, p. 194-195).

La tercera peculiaridad proveniente de la inseguridad que se desarrolla en el dominio cibernético. Kallberg y Cook (2017), al tratar de los retos del espacio cibernético para el pensamiento militar tradicional, indican que el anonimato y la dificultad de mensurarse el impacto de un ataque cibernético son elementos que corroboran para el predominio del principio de la inseguridad inherente al dominio cibernético. Dada su naturaleza interconectada y altamente compleja, un eventual ataque es difícilmente cuantificado o es mensurado, ya que los efectos no son, necesariamente, cinéticos y/o inmediatos, estando muchas veces escondido debajo de inúmeras camadas de red semánticas y sintácticas.

El anonimato, a su vez, puede ser utilizado como herramienta tanto de protección cuanto de ataque. Tal característica puede tener como consecuencia la identificación errónea de un ataque cibernético, ocasionando un eventual contra-ataque a inocentes, llevando a la escalada descontrolada del conflicto. La llegada del nuevo dominio eleva el "derrotar el enemigo sin luchar" y el "hacer a los otros luchar sus batallas" a otro nivel.

La combinación de los elementos de desterritorialidad, difusión de poder e inseguridad permite que nuevas y antiguas amenazas accionen en el espacio cibernético, realizando un objetivo de actos que van desde la diplomacia al sabotaje, espionaje, monitoreo y mismo a ataques con efectos cinéticos. El espacio cibernético se consagra, de esa manera, como escenario para todos los tipos de actores y amenazas.

Como ejemplo, Edward Snowden – entonces analista de la Agencia de Seguridad Nacional Norte Americana (NSA) –, en el año de 2013, en alianza con periodistas de distintos países reveló el programa de espionaje y monitoreo ejercido por NSA. Países como Brasil, Alemania y Francia tuvieron jefes de Estado, miembros del gobierno y empresas monitoreadas por la agencia norte americana, con el auxilio de países aliados pertenecientes al llamado grupo "Cinco Ojos", compuesto por agencias de seguridad de Estados Unidos, Canadá, Australia, Nueva Zelandia y Reino Unido, que trabajaban en conjunto, monitoreando a ciudadanos alrededor del globo (BRIDI; GREENWALD, 2013; WIKILEAKS, 2015; PRIVACY INTERNATIONAL, 2015).

Proveniente del espionaje en Brasil, es pertinente el habla de Celso Amorim (2013, p. 289), con respecto del continuo estrechamiento de la línea que separa el espionaje en línea y la guerra cibernética desde características como la inseguridad en el ciberespacio:

> El monitoreo de datos y la guerra cibernética tienen en común el empleo de instrumentos de altísima tecnología para actividades que importan en graves violaciones de soberanía. Cuando el objeto del monitoreo va más allá de la mera observación, y tiene

> el objetivo de la toma de conocimientos tecnológicos, la frontera entre el espionaje y la guerra queda todavía más difícil de ser determinada. Conceptualmente, no habría diferencia, salvo tal vez en el que se refiere a daños inmediatos, entre un acto de espionaje, de búsqueda de informaciones económicas y tecnológicas, y un ataque tradicional para la obtención de un recurso económico.
>
> El monitoreo y la guerra cibernética pueden disparar tanto países que son tenidos como hostiles o como amenazas inmediatas cuanto países amigos y aliados. Ya sabemos que ese fue el caso en la interceptación de datos. No se puede excluir que el mismo ocurra con ataques cibernéticos, provenientes de cualquier cuadrante. Esas dos actividades ilustran en tonos muy fuertes algunos de los nuevos retos de la seguridad internacional.

El monitoreo expuesto por Snowden representa la excepción la regla, ya que debido a la multiplicidad de actores y anonimato en el ciberespacio es improbable identificar con precisión la actuación de actores nacionales. No obstante, es posible vislumbrar la actuación de actores estatales en el espacio cibernético, sin que ocurra una confirmación o reconocimiento oficial.

Quizá uno de los ejemplos más emblemáticos sea el caso Stuxnet. Se trata de un *malware* que contaminó los ordenadores de centrífugas nucleares de Irán, saboteando el proyecto nuclear del país. Todos los indicios indican para un ataque cibernético que fue realizado por Estados Unidos en conjunto con Israel para atrasar el programa nuclear de aquel país. No obstante, estadunidenses y/o israelíes nunca asumieron de hecho la autoría del ataque (KENNEY, 2015).

El monitoreo o el sabotaje cibernético que fue realizado por otros Estados, constituye "antiguas amenazas" en el sentido de que siempre hubo espionaje, sabotaje y guerras entre países. No obstante, estas se tornan "antiguas amenazas" en el ciberespacio desde el momento que la difusión de poder las obliga a actuar paralelamente con otros agentes.

En el que se refiere a las nuevas amenazas del espacio cibernético, se tienen aquellas no solo estimuladas por estados para los fines que fueron mencionados arriba, sino también, las amenazas que fueron promocionadas por actores no estatales. O sea, son traspasadas las amenazas del nivel estatal para el nivel de los individuos. Estos, por ejemplo, pasan a ser capaces de desestabilizar gobiernos mediante la realización de ataques con las más variadas motivaciones. De entre las amenazas no estatales pueden ser indicados el activismo cibernético, el crimen cibernético y el terrorismo cibernético.

El activismo cibernético es caracterizado como la mezcla entre las acciones *hacker y* el activismo político, de forma a inviabilizar servidores o sitios electrónicos (CEPIK; CANABARRO; BORNE, 2014). Se puede decir, todavía, que el ciberactivismo se involucra en cuestiones volcadas a determinadas causas desde la realización de ataques a los gobiernos y empresas que se presentan en contradicción con sus ideas, de manera a inducirlos a reevaluar sus decisiones institucionales, con el fin de llamar la atención del público a la causa defendida (ZUCCARO, 2012).

Definido como acto u omisión cometida en violación a una ley en el espacio cibernético, el crimen cibernético se presenta como una actividad criminal que es relacionada a la invasión ilegal a los ordenadores, a la manipulación de informaciones, al sabotaje de equipos y al robo de datos (SAINI; RAO; PANDA, 2012). De manera más amplia, se puede decir que el ciberdelincuencia es el desarrollo de acciones ilícitas a ser aplicadas en sistemas y redes de ordenadores. Utilizándose del espionaje cibernético para probar configuraciones y sistemas de defensa con el objetivo de tener

acceso a informaciones secretas, cibercriminales pueden realizar sabotajes cibernéticos al generar obstáculos por medios electrónicos (CEPIK; CANABARRO; BORNE, 2014).

El ciberterrorismo, aunque no poseyendo una definición ampliamente aceptada – teniendo como objetivo la variación del término componente terrorismo – (CHEN, 2014), es interpretado, de manera general, como acciones realizadas por actores no estatales contra redes y sistemas de ordenadores, capaces de resultar en violencia contra civiles. En lo más, los ataques deben contener motivación política y generar daños físicos además de virtuales (POLLIT, 1998; WEIMANN, 2005; KENNEY, 2015). Según Dorothy Denning (2000), amenazas cibernéticas contra ordenadores, redes y sistemas indican la búsqueda por intimidación de los gobiernos y de las poblaciones, anhelando el alcance de objetivos sociales y políticos de grupos e individuos. Además de eso, el ciberterrorismo tiene el objetivo de una amplia escala de exhibición y publicidad, así como en el terrorismo tradicional (COLLIN, 1997).

Independiente de las motivaciones de determinadas amenazas, es percibido que el espacio cibernético se demuestra cómo ambiente en el cual distintas acciones son realizadas con variables niveles de éxito. La interconectividad mientras aproxima a las personas y permite una amplia variedad de actividades y facilidades antes inimaginables, abre también puertas para amenazas hace poco impensables. Luego, diversos Estados perciben la importancia de la seguridad y defensa cibernética nacionales, una vez que ataques de esa naturaleza pueden generar daños físicos, políticos, económicos y sociales irremediables.

3 **La titulización del ciberespacio**

El escenario internacional posGuerra Fria inició la discusión de nuevos temas en la agenda internacional que pasaron a ganar mayor relevancia en los años 1990, tornándose necesaria la introducción de nuevos modelos de análisis de seguridad (FARRET, 2014). Por la insuficiencia del debate teórico-epistemológico del período, la producción, antes concentrada en cuestiones estado céntricas, se amplió para análisis de actores no estatales e individuales, demostrando que el sistema internacional debería ser analizado no solamente a través de las relaciones interestatales. Así, conceptos hasta entonces considerados inmutables pasaron a ser redefinidos (BUZAN; HANSEN, 2012).

Basada en las premisas de la corriente constructivista, la Escuela de Copenhague desarrolla el concepto teórico de titulización. Comprendiendo el alargamiento del campo de la seguridad internacional, la Escuela amplia el concepto de seguridad para más allá del dominio político-militar al introducir nuevos sectores de análisis: el económico, el ambiental y el social. Para eso, se utiliza del análisis de los discursos y de las unidades de seguridad para certificar la titulización de determinado tema.

Por medio de la teoría de titulización, nuevas maneras de análisis de seguridad pasaron a ser consideradas por intermedio de los discursos y del posicionamiento de agentes no-estatales e individuales en el sistema internacional. Así, nuevas amenazas internacionales, anteriormente conectadas esencialmente al Estado, pasaron a ser mejor percibidas y entendidas (MOTTA, 2014). Ese aspecto posibilitó que los estudios fueran extendidos para la seguridad de los individuos y demostró casos en que el Estado y la sociedad no se equilibran como, por ejemplo, cuando minorías nacionales son amenazadas por el propio Estado o, cuando este moviliza la sociedad para la confrontación de amenazas internas o externas (BUZAN; HANSEN, 2012).

De acuerdo con Grace Tanno (2003), los procesos de construcción de seguridad se inician desde discursos que fueron realizados por actores interesados en establecer las agendas de seguridad, pudiendo, de esa forma, sufrir el proceso de titulización. No obstante, tal proceso no depende solamente de los agentes titulizados como, también, necesita que la propuesta sea reconocida socialmente como una amenaza a la seguridad. En otras palabras, para que sea creada una situación de seguridad desde el discurso, es preciso que la audiencia la cual él se dirige y la cual requisita los medios necesarios para el objeto que vendrá a ser titulizado concorde voluntariamente con el discurso, direccionando el acto de titulización (AMARAL, 2008).

Por lo tanto, se entiende por titulización el proceso en el cual el Estado es amenazado existencialmente, siendo necesarias acciones emergenciales que pueden, incluso, sobrepasar leyes y procedimientos políticos (BUZAN; WEAVER; WILDE, 1998). Luego, titulización cibernética puede ser interpretada como el proceso de acción de emergencia contra una amenaza en potencial en el espacio cibernético. Son considerados actores del ambiente cibernético los estados, las instituciones, las corporaciones industriales y empresariales, los sectores financieros y de servicios, grupos de activistas políticos y religiosos, criminales digitales, entre otros. La variedad y cuantidad de actores se multiplican en la medida en que avanza la tecnología y el acceso a la información. De entre esos actores, pueden ser observados tanto aquellos que irán promover el discurso de titulización, como los actores que pueden ser considerados amenazas a la seguridad estatal.

El proceso de titulización es mejor vislumbrado en el sector militar, una vez que el monopolio de la fuerza del estado moderno lo convierte legítimo para la protección nacional delante de amenazas a la seguridad nacional. De esa manera, el Estado es considerado el objeto de referencia, mientras que las elites militares son los actores de titulización que son responsables por la determinación de las acciones a las amenazas mediante los actos de habla (TANNO, 2003). El proceso de titulización se torna evidente en el momento en que el ciberespacio es reconocido por los documentos de defensa como un dominio estratégico en el cual emanan distintos amenazas.

La extensión de las amenazas y de las vulnerabilidades irá a variar de acuerdo con las capacidades relativas y absolutas de los involucrados (BUZAN; WEAVER; WILDE, 1998). Mientras tanto, cuando llevado al ámbito cibernético, la asimetría de capacidades y la creciente vulnerabilidad de las infraestructuras críticas transforman la naturaleza de la amenaza, una vez que las peculiaridades inherentes al ciberespacio dificultan la prevención contra los ataques cibernéticos.

El ciberespacio amplia las formas con las cuales se puede afectar la estabilidad organizacional del Estado; la organización de la primavera árabe dispensa mayores comentarios. Acciones cibernéticas con motivaciones políticas[6] que tienen el objetivo de desestabilizar el gobierno de manera a divulgar determinado ideal pueden ocasionar daños a otros sectores de la sociedad, tornando la titulización más compleja y sensible. Todavía, pueden ocasionar la pérdida de legitimidad interna y externa de un Estado caso no se proponga a titulizar el sector político contra las amenazas cibernéticas.

6 Las amenazas políticas pueden ser clasificadas como amenazas intencionales – cuando un Estado no reconoce la legitimidad de un Estado/gobierno extranjero o el gobierno es rechazado por un grupo en el ámbito doméstico por conflictos de principios distintos – y amenazas estructurales – cuando hay contradicciones en los principios organizacionales del Estado (TANNO, 2003). Consonante Buzan, Weaver y Wilde (1998), las amenazas existentes en el sector político a un Estado son aquellas que desafían la soberanía nacional, una vez que una amenaza en el ámbito político puede ser transferida para los otros sectores (BUZAN; WEAVER; WILDE, 1998).

Las amenazas económicas pueden ser consideradas como aquellas "dirigidas a los sectores económicos que garanticen la supervivencia del Estado y que son fundamentales en el esfuerzo de guerra" (TANNO, 2003). Con el objetivo de la interdependencia, amenazas la estabilidad económica de un Estado pueden ser entendidas como globales (BUZAN, WEAVER, WILDE, 1998). De esa manera, las amenazas cibernéticas que tienen el objetivo de ganancias económicas mediante robo de informaciones bancarias – tanto en la escala del individuo como empresarial o estatal, por ejemplo – pueden ocasionar daños económicos y financieros al Estado, además de transferir esos daños para otros sectores interconectados.

Por fin, aunque no tratando especificadamente de la revolución de la información en el estudio de seguridad, la Escuela de Copenhague presenta, por intermedio de la teoría de titulización, como, cuando y cuales consecuencias los actores políticos perciben como amenaza existencial a la seguridad desde los actos de habla – o discursos políticos –, creando una agenda de seguridad de emergencia. El universo cibernético amplia la variedad de amenazas que pasan a ser, incluso, menos perceptibles, por cuenta de las cuestiones de anonimato e inseguridad que fueron mencionadas anteriormente. Esas peculiaridades del nuevo dominio inician nuevos abordajes en el proceso de titulización.

4 El ciberespacio en los libros blancos de defensa

Considerando el eventual desfasaje entre las medidas de seguridad y de defensa nacional en relación al acelerado avance de la tecnología, los Estados pasan a preocuparse en proteger y reducir sus vulnerabilidades por medio de medidas capaces de promover algún tipo de desarrollo estatal en el ámbito de la seguridad, específicamente en relación a la cibernética. Delante de la nueva arena de poder que el espacio cibernético representa, es analizado el proceso de titulización en los libros blancos de defensa de la Alemania, Francia y Brasil mediante el reconocimiento del ciberespacio como dominio estratégico.

Alemania

En el Libro Blanco de la Política de Seguridad Alemana y el Futuro de las fuerzas Armadas (*White Paper on German Security Policy and the Future of the Bundeswehr*), editado en 2016, son presentados los retos para la política de seguridad del país. En la esfera de las amenazas se encuentran la cuestión del terrorismo, de las armas de destruición en masa, del descontrol de migración, conflictos interestatales, control climático, entre otros. Tratando específicamente del dominio cibernético, hay una clara preocupación con las vulnerabilidades del Estado frente a posibles ataques cibernéticos. Sobre el tema, el documento afirma ser necesarias "medidas urgentes para la protección contra amenazas" (GERMANY, 2016, p. 36, nuestra traducción).

El documento alemán no ofrece una definición clara sobre seguridad cibernética. Mientras tanto, presenta el concepto de dominio de la información como el espacio en el cual las informaciones son generadas, procesadas, diseminadas, discutidas y almacenadas. De acuerdo con el Libro Blanco de la Política de Seguridad Alemana, el espacio cibernético es tenido como espacio virtual de todos los sistemas de la Tecnología de la Información vinculados o vinculables en escala global.

Es indicado, en el documento, la gravedad de los ataques cibernéticos a las infraestructuras críticas que pueden generar consecuencias a la población civil, exponiendo que los efectos de los ataques no pueden ser resueltos en un futuro previsible, una vez que la tendencia es que esa

cuestión sigue a agravarse. Todavía, es presentado que la cibernética y el dominio de la información son áreas de importancia estratégica e internacional, siendo necesaria la mejora del tiempo de respuesta como prevención a los ataques cibernéticos y operaciones de información, poniendo como prioridad la protección y la defensa cibernética.

> Debemos tomar medidas preventivas para reducir ese riesgo por medio de mecanismos de construcción de confianza y resolución de conflictos.
> Hay pocas áreas en que la seguridad interna y externa están tan estrechamente entrelazadas cuanto en el espacio cibernético. La situación de amenaza en el espacio cibernético exige un abordaje holístico en el ámbito de la política de seguridad cibernética (GERMANY, 2016, p. 38, nuestra traducción).

En relación al sector cibernético, el Libro Blanco de la Política de Seguridad Alemana prioriza la necesidad de reducir las vulnerabilidades de las infraestructuras críticas nacionales, como sistemas de comunicación, energía y logística. En lo que se refiere a las amenazas consideradas en el documento, es presentada preocupación en relación a ataques de actores no estatales, como grupos terroristas, crimen organizado, además de individuos especializados que podrían ocasionar serios daños con mínimos esfuerzos. Tales amenazas confirman la preocupación con actos que pueden ser provocados por agentes no estatales. Así, individuos son percibidos como actores internacionales, conforme análisis del documento alemán. Tal hecho, por sí solo, iniciaría densa discusión teórica relativa a las relaciones internacionales, el que va mucho más allá en los propósitos y en límites del presente artículo.

El documento no presenta, específicamente, la relación del espacio cibernético con la esfera civil, sino deja claro la importancia de la transparencia entre los sectores público y privado y la necesidad de cooperación con otros estados. Conforme el Libro Blanco de la Política de Seguridad Alemana, solamente por medio de una política de seguridad cibernética y una política externa cibernética sería alcanzada una efectiva protección contra cibercriminales y ataques cibernéticos. Las informaciones que han sido obtenidas en el documento son enumeradas en la tabla la seguir.

Tabla 1 - Sumario de las informaciones que fueron obtenidas en el Libro Blanco de la Política de Seguridad Alemana

Año de edición	2016
¿Hay alguna definición clara de seguridad cibernética en los documentos?	No
¿Lo que esos documentos exprimen sobre el sector cibernético?	Área de importancia estratégica e internacional. Es priorizada la protección y defensa cibernética.
¿Cuáles son las amenazas consideradas?	Actores no estatales. Grupos terroristas, crímenes organizados, individuos especializados en daños infraestructurales.
¿Cuál es el posicionamiento en relación al involucramiento de otros sectores civiles?	No especifica, sino afirma la necesidad de transparencia entre los sectores para el combate de las amenazas cibernéticas.

Fuente: Basado en Germany (2016)

Alemania atribuye el surgimiento de nuevas amenazas como uno de los factores que llevó a la necesidad de reformulación de su Libro Blanco, argumentando que "nuevas amenazas y peligros surgieron además de aquellos que ya existían" (GERMANY, 2016, p. 15). En el que se refiere a las amenazas oriundas del dominio cibernético, hay una sesión dedicada, exclusivamente, al combate a "Amenazas a los sistemas de información y comunicación, líneas de provisión, rutas de transporte y comercio, así como al suministro seguro de materias primas y energía" (GERMANY, 2016, p. 41). En esa sesión, la prosperidad de la sociedad alemana es tenida como dependiente del uso de comunicaciones e informaciones globales, y cualquier "interrupción del acceso a esos bienes públicos globales en tierra, en el aire, en el mar, en el dominio cibernético y de la información y en el espacio involucra riesgos considerables para la capacidad de nuestro estado funcionar y para la prosperidad de nuestros ciudadanos" (GERMANY, 2016, p. 41).

El texto sostiene la necesidad de perfeccionamiento de personal y tecnología para mejor actuación estatal en el ciberespacio. Tal vez, como consecuencia, en abril de 2017, fue creado el Cyber and Information Space Command (CIR), que corresponde al brazo cibernético de las fuerzas armadas alemanas (WERKHÄUSER, 2017).

Francia

En el análisis del Libro Blanco de la defensa y Seguridad Nacional Francesa (French White Paper on Defence and National Security), que fue elaborado en 2013 por el gobierno francés, es constatada la preocupación con ataques cibernéticos – juntamente con amenazas de proliferación nuclear, pandemias y terrorismo –, luego en las primeras líneas del prefacio que fue escrito por el entonces presidente François Hollande.

El documento considera la creciente inserción de la sociedad francesa en los medios de comunicación como una forma de vulnerabilidad. En ese sentido, resalta que el acceso universal al ciberespacio y la no identificación de responsables (luego, la cuestión de la inseguridad, que fue discutida anteriormente) son sus principales agravantes. En el contexto, son aludidas las amenazas en el ciberespacio, desde cibercriminales a ataques cibernéticos que eran encabezados por otras naciones. Por esas colocaciones, se visualiza en el Libro Blanco francés que el ciberespacio es entendido como ambiente esencial al Estado, escenario de retos y conflictos en potencial. "La posibilidad de un gran ciberataque en sistemas nacionales de información en un escenario de guerra cibernética constituye una amenaza extremamente grave para Francia y los sus aliados europeos" (FRANCE, 2013, p. 43).

En relación a las preguntas que componen el análisis comparativo propuesta en este artículo, el Libro Blanco de la defensa y Seguridad Nacional Francesa no ofrece una definición clara de seguridad cibernética. Sin embargo, interpreta el ciberespacio como área de conflictos y el considera una prioridad estratégica en relación a la protección contra amenazas y ataques. En relación a las amenazas, son considerados tanto agentes no estatales cuanto Estados que pueden desarrollar espionaje y ataques cibernéticos. Con respecto de la introducción del sector civil como auxilio para la protección nacional, el documento, a pesar de involucrar otros sectores del gobierno – además de las fuerzas Armadas –, no trata la cuestión del involucramiento civil. La tabla 2 presenta una síntesis de las informaciones que fueron obtenidas.

Tabla 2 - Sumario de las informaciones que fueron obtenidas en el Libro Blanco de la defensa y Seguridad Nacional Francesa

Año de edición	2013
¿Hay alguna definición clara de seguridad cibernética en los documentos?	No
¿Lo que esos documentos exprimen sobre el sector cibernético?	El ciberespacio es considerado área de confronto y de amenazas. Es percibido como prioridad estratégica desde la protección contra ciberataques.
¿Cuáles son las amenazas consideradas?	No estatales, como cibercrimen y terrorismo a las empresas estatales. Considera la posibilidad de ataques cibernéticos en un escenario de ciberguerra.
¿Cuál es el posicionamiento en relación al involucramiento de otros sectores civiles?	A pesar de involucrar otros sectores del gobierno, además de las fuerzas Armadas, no trata la cuestión del involucramiento civil.

Fuente: Basado en France (2013)

En el caso de Francia, no son consideradas nuevas amenazas específicamente. Eso se debe, de acuerdo con el Libro Blanco francés, al hecho de que las amenazas aludidas en el documento ya haber sido abordadas en la versión anterior, que fue publicada en 2008. No obstante, el documento trata, en su introducción, de la diseminación de riesgos y amenazas. Entre ellas, el terrorismo, ciberamenazas, crimen organizado, la proliferación de armas convencionales y nucleares. Riesgos pandémicos, tecnológicos y naturales son tenidos como cuestiones estratégicas que pueden tener consecuencias dañosas para Francia (FRANCE, 2013, p.10).

El Libro Blanco de Francia presenta una sesión específica al combate a ciberamenazas, que, conforme el texto, se tornan prominentes conforme la sociedad francesa pasa a depender más de sistemas informacionales interconectados. La capacidad de protegerse contra ataques cibernéticos es tratada como una cuestión de soberanía nacional. Así, como el documento alemán, el Libro Blanco francés enaltece la necesidad de desarrollo de personal y capacidades para operación en el ciberespacio. Tal como en el caso alemán, no hay cualquier mención a la idea de creación del COMCYBER, unidad de guerra cibernética que se tornó operativo tres años después de la publicación del Libro Blanco francés (REEVE, 2016).

Brasil

La transversalidad entre las nuevas y las tradicionales amenazas indicaron la necesidad de adecuación de los nuevos temas a la realidad brasileña. Con interés en promocionar transparencia y diálogos entre las instituciones nacionales, la sociedad y la comunidad internacional en el ámbito de la defensa, el Libro Blanco de defensa Nacional (LBDN) brasileño propone ser un mecanismo de cooperación entre los países de Suramérica.

En ese sentido, el sector cibernético fue incluido al documento en el status de prioridad estratégica nacional, juntamente con los sectores nuclear y espacial. La incorporación del sector al LBDN se relaciona con la creación del Libro Verde: Seguridad Cibernética en Brasil, que fue publicado en 2010. Preliminarmente, fue elaborado en la intención de ser referencia para la creación de un "Libro Blanco: Política Nacional de Seguridad Cibernética", el documento presenta directrices estratégicas nacionales de ciberseguridad, así como indica esfuerzos de cooperación y diálogo internacional, principalmente en el ámbito de la *Organization for Economic Co-operation and Development* (OCDE).

El Libro Verde designa y elucida los principales sectores estratégicos brasileños en niveles de oportunidades y retos que involucran la seguridad cibernética, siendo ellos: político-estratégico, económico, social y ambiental, CT&I, educación, legal, cooperación internacional y seguridad de las infraestructuras críticas. Por medio de estos, propone una macro-coordinación entre sectores e inter-agencias que actúan en la esfera de la ciberseguridad, con la finalidad de fortalecer el espacio cibernético brasileño. El referido documento deja claro también que el desarrollo de estrategias y normas aseguran el crecimiento de incentivos la investigación e innovación, generando la capacitación de recursos humanos, mayor protección de las infraestructuras críticas y cooperación nacional e internacional.

Vislumbrando la estructuración de la seguridad cibernética en Brasil, el Libro Verde presenta como propuesta de agenda iniciativas para

> [...] apoyar y fortalecer sus actividades, de manera a viabilizar y agilizar tanto la formulación de políticas, normas y regulación, la investigación y el desarrollo de metodologías y tecnologías, cuanto a la cooperación internacional y la implantación y promoción de una macro-coordinación que propicie la integración de procesos, con el objetivo de asegurar la disponibilidad, la integridad, la confidencialidad y la autenticidad de las informaciones de interés del Estado brasileño y de la sociedad, así como la resiliencia de sus infraestructuras críticas (BRASIL, 2010, p. 25).

Por más que el Libro Verde no haya concretado el objetivo de lanzar la política nacional de ciberseguridad, posibilitó la apertura de la planificación estratégica nacional de seguridad cibernética para la Estrategia Nacional de defensa (END), para la Política Nacional de Defensa (PND) y, luego, para el LBDN. Los apuntes que fueron propuestos alcanzaron el nivel de fomentar la protección y el desarrollo del ciberespacio brasileño, principalmente al evidenciar la relevancia que las demás naciones confieren al tema. De esa forma, el interés en atribuir importancia al sector cibernético se tradujo en determinar premisas para un proyecto de ciberdefensa y presentar esfuerzos de actuaciones interagencias, conforme indicado en el LBDN de 2012. Para eso, el Libro Blanco designa como responsabilidad del Ejército Brasileño la defensa del espacio cibernético[7].

En el ámbito de la coordinación del Ejército, son indicados los avances en la capacitación de recursos humanos, así como la competencia de accionar y proteger el ciberespacio. De modo a estimular el avance y las innovaciones tecnológicas para la base industrial de defensa, el LBDN indica para la construcción de sistemas y de componentes críticos nacionales. Además de eso, el documento presenta el Centro de defensa Cibernética del Ejército (CDCiber) como el agente responsable por fortalecer la seguridad, poseer la libertad de acción de respuesta a incidentes cibernéticos, capacitar recursos humanos y proteger el ciberespacio brasileño. Para tales fines, el CDCiber acciona en conjunto con otros órganos gubernamentales que abarcan el sector.

La inserción del sector cibernético al ámbito de sectores estratégicos de defensa es presentada en el LBDN en la forma de "conferir confidencialidad, disponibilidad, integridad y autenticidad a los datos

7 Conforme los más altos documentos de defensa de Brasil (LBDN, PND y END) hay tres sectores estratégicos para la defensa nacional: cibernético – bajo responsabilidad del Ejército –; nuclear – bajo responsabilidad de la Marina – y espacial, bajo responsabilidad de la Fuerza Aérea.

que transitan en sus redes, los cuales son procesados y son almacenados" (BRASIL, 2012, p. 71). Además de demostrar ser un objetivo a largo plazo, el documento también indica para acciones a ser ejecutadas en el corto plazo, considerando el dinamismo que el sector posee. Son ellas: i) construcción de la sede del CDciber; ii) adquisición de infraestructura, equipos de apoyo y soluciones de *hardware* y *software* de defensa; iii) capacitación de recursos humanos y; iv) proyectos que estructuren el sector cibernético.

Se tiene, por lo tanto, que el LBDN expone de forma abarcadora los indicativos y las competencias que se atribuyen al sector cibernético. En cuestiones de conceptos y definiciones, no fueron especificados los temas que comprenden el alcance del espacio cibernético, dificultando la congruencia de informaciones y formulaciones de los términos para la actuación de los órganos responsables. No solamente, no fueron identificadas las amenazas que son ofrecidas al ciberespacio brasileño. En relación a la actuación de otros actores en la defensa cibernética, el LBDN menciona solamente la participación de órganos gubernamentales que ya poseían alguna conexión con el sector.

Es importante subrayar, todavía, que la primera edición del Libro Blanco de Defensa Nacional brasileño fue publicada en 2012; la segunda edición, de 2016, solamente sería aprobada en diciembre de 2018 por el Congreso Nacional[8]. El presente artículo utilizó como fuente la versión de 2012 y la minuta del documento de 2016, aprobada en su totalidad por el Congreso[9]. Delante de la capilaridad de las tecnologías de información y comunicación en la sociedad brasileña, la minuta del LBDN de 2016 alerta para los retos que son puestos al país por la naturaleza híbrida o irregular de los "conflictos del futuro", que aglutinan acciones de combate regular con elementos informacionales y cibernéticos, pudiendo ser realizado por actores estatales y no estatales. El surgimiento de guerras cibernéticas, de manera general, también es tenido como un reto para la defensa brasileña.

En la minuta del LBDN, se tiene que la "amenaza cibernética se convirtió una preocupación, por poner en riesgo la integridad de infraestructuras sensibles, esenciales a la operación y al control de diversos sistemas y órganos directamente relacionados a la seguridad nacional" (BRASIL, 2016. p. 57). Aun así, el LBDN no caracteriza específicamente el que sería amenaza cibernética. No obstante, el sector cibernético, en conjunto con el nuclear y el espacial, se mantienen considerados estratégicos y prioritarios para la defensa nacional.

El documento de 2016 todavía no ofrece una definición clara sobre el que sería seguridad cibernética. El ciberespacio es tenido como prioridad desde el momento que, por intermedio de él, se puede causar daños a infraestructura y la sociedad que está cada vez más insertada en las tecnologías de información y comunicación. En relación a las amenazas, el documento comenta brevemente sobre la posibilidad de ataques que fueron cometidos por agentes estatales y no estatales, sin embargo, no se profundiza en la identificación o caracterización de estos. Por fin, con respecto del involucramiento con el sector civil, el LBDN además de tornar el Ejército Brasileño responsable por la defensa del espacio cibernético, involucra otros sectores del gobierno y militares, considera la participación en foros internacionales, y trata la cuestión del involucramiento civil, mediante el acercamiento de las Fuerzas Armadas con el sector privado y la academia.

8 El decreto legislativo PDS 137/2018 que aprobó las nuevas directrices para la Política Nacional de Defensa (PND), para la Estrategia Nacional de Defensa (END) y la actualización del Libro Blanco de la Defensa Nacional (LBDN) fue publicado en el Diario Oficial de la Unión el 17 de diciembre de 2018.

9 Para un análisis profundizado de los documentos de defensa de Brasil y de otros países de Suramérica, consultar la obra "Guía de Defensa Cibernética en Suramérica" de Oliveira et al (2017).

De esa manera, es posible visualizar en los documentos de defensa que fueron presentados que los esfuerzos en promocionar regulaciones y objetivos claros para la actuación en el sector cibernético se encuentran en etapa inicial. Por lo más que, en el intervalo entre los días actuales y el LBDN de 2012, haya sido presentada la minuta del LBDN en 2016, es demostrada poca evolución en cuestiones de objetivos, metas y aspiraciones entre ellos. Considerando el dinamismo que el espacio cibernético ofrece y la velocidad que las amenazas se transforman en el mundo contemporáneo, se llama la atención para la necesidad de tornar los mecanismos efectivos en el combate a los ataques cibernéticos, así como los documentos influir con claridad las especificidades de actuación para el órgano responsable.

Tabla 3 - Sumario de las informaciones que fueron obtenidas en el Libro Blanco de Defensa Nacional (LBDN)[10]

Año de edición	2016 (minuta)
¿Hay alguna definición clara de seguridad cibernética en los documentos?	No
¿Lo que esos documentos exprimen sobre el sector cibernético?	El sector cibernético es visto como prioritario, pues por intermedio del ciberespacio se puede causar daños a la infraestructura
¿Cuáles son las amenazas consideradas?	Estatales y no estatales. No hay una mayor profundidad sobre cuáles serían esas amenazas.
¿Cuál es el posicionamiento en relación al involucramiento de otros sectores civiles?	Involucra otros sectores del gobierno y militares, considera la participación en foros internacionales, pero no trata del involucramiento civil.

Fuente: Basado en Brasil (2016)

La versión más reciente del LBDN brasileño determina el establecimiento del Comando de Defensa Cibernética (ComDCiber) como organización militar conjunta, en la cual están subordinados el CDCiber y la Escuela Nacional de Defensa Cibernética (ENaDCiber). La creación del ComDCiber "tiene como principales atribuciones, de entre otras, planificar, orientar, supervisar y controlar las actividades operativas, de inteligencia, doctrinaria, de ciencia y tecnología, así como de capacitación en el Sector Cibernético de Defensa" (BRASIL, 2016, p. 58). En ese punto, es identificada una progresión institucional de la cuestión cibernética en los documentos brasileños, en consecuencia de la creación de un comando más abarcador y por lo tanto, más capacitado jerárquicamente en términos de personal, recursos e infraestructura que el CDCiber, como lo establecido por la versión del LBDN de 2012.

La creación del ComDCiber evidencia, por lo tanto, una evolución en la percepción del valor estratégico que es atribuido al sector cibernético por el gobierno brasileño como agente de titulización. No obstante, es importante subrayar que no se trata de una ramificación de las Fuerzas Armadas como ocurre con el CIR alemán y el COMCYBER francés.

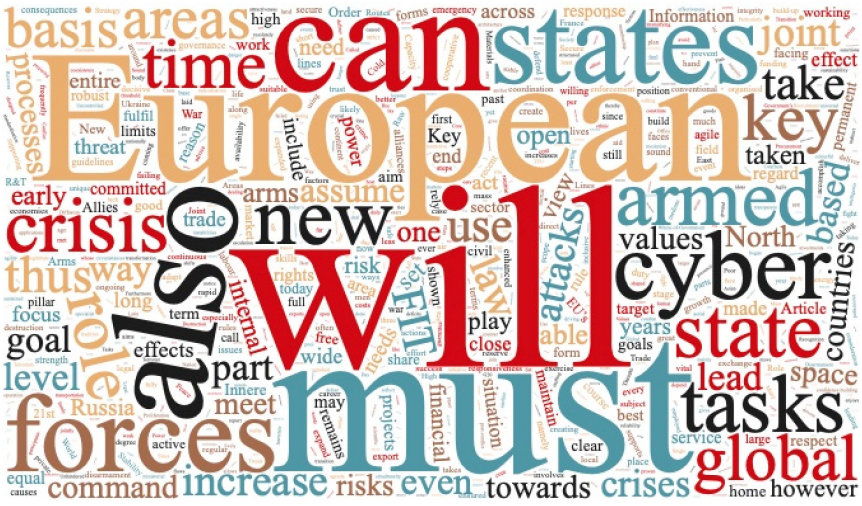
5 **Análisis comparativo de los documentos**

En lo que se refiere al análisis comparado de los contenidos de los documentos, se buscó evidenciar los variados niveles de prominencia atribuidos por los Estados en cuestión a temas específicos.

10 A pesar de en el presente artículo ser abordadas tanto las ediciones de 2012 cuanto de 2016, por cuestiones metodológicas, el análisis sumario se restringe al último documento, o sea, la versión más reciente del LBDN que fue publicado por Brasil, tal como ocurrió en los análisis de Alemania y Francia.

Con el intuito de evidenciar la prominencia de determinados temas en los documentos, fue hecho el análisis de conteo automatizado del número de hechos de palabras en cada Libro Blanco, resultando en la agregación de palabras a continuación.

Figura 1 - Agregación de palabras del Libro Blanco de Defensa de Alemania



Fuente: Basado en Germany (2016)

Es notable la preminencia del contexto europeo en relación al nacional. Se observa, todavía, que la temática cibernética aparece con significada frecuencia en el texto. Eso ocurre debido a la utilización amplia del prefijo "cyber" a lo largo del libro, empleado para referirse a "ciberamenazas", "ciberataques", "ciberespacio", entre otros.

La figura 2 presenta graficamente las palabras y temas más presentes en el documento frances.

Figura 2 - Agregación de palabras del Libro Blanco de Defensa de la Francia

Fuente: Basado en France (2013)

Sin mayores profundizajes, se percibe, rapidamente, la sustitución del término "european", destaque en el análisis del documento alemán, por la palabra "world", en el texto francés. El término "cyber" no posee en el documento francés la misma preminencia certificada en el documento alemán. La agregación de palabras oriunda del Libro Blanco francés evidencia un discurso más imperativo, cuando es comparado al documento alemán, mientras que la temática de amenazas aparece de manera más preminente a lo largo del texto.

Figura 3 - Agregación de palabras del Libro Blanco de Defensa de Brasil[11]

Fuente: Basado en Brasil (2016)

La aglomeración de palabras en la minuta de 2016 evidencia la preminencia de la participación militar en la defensa, cuando comparada a los otros países. Mientras los demás libros blancos no llegan a distribuir atribuciones para distintos fuerzas o sectores civiles, la minuta del LBDN es objetivo y categórico, manteniendo las áreas de responsabilidad para cada ramo de las Fuerzas Armadas y determinando la creación del ComDCiber.

Dando continuidad al análisis comparativo, fue desarrollada la tabla 4 que trata sobre la cuantidad de páginas totales de los documentos, el número de páginas que tratan la cuestión de las amenazas, nuevas amenazas y específicamente la cuestión cibernética.

Tabla 4 - Comparativo de páginas entre los libros blancos

	Total de Páginas	Páginas dedicadas a amenazas	Páginas dedicadas a nuevas amenazas	Páginas dedicadas a la cuestión cibernética
Alemania	143	24	1	28
Francia	135	52	0	23
Brasil	185	12	1	15

Fuente: Basado en France (2013), Brasil (2016) y Germany (2016).

11 La incidencia de preposiciones se debe a dos factores: las peculiaridades de la lengua portuguesa y la imposibilidad de exclusión de términos en la herramienta de análisis empleada.

Como observado en el análisis específico de cada país, la categorización de "nuevas amenazas" es casi inexistente, de manera que ocurre la disparidad del número de páginas que abordan la temática de las "nuevas amenazas" y de las "amenazas". Eso se da en consecuencia del tratamiento dado las amenazas no estatales, que a pesar de su originalidad en el dominio cibernético, son categorizadas como amenazas por los documentos de defensa. Hecho que indica una madurez del discurso de titulización de los países y desentona de la concepción de amenazas única y exclusivamente estatales.

Otro punto relevante corresponde al número mayor de páginas para la cuestión cibernética en relación a las amenazas, elemento que condice con la interpretación vigente en los documentos de que el ciberespacio no es solamente el espacio para amenazas, sino también un dominio estratégico para el desarrollo de los países en cuestión.

El abordaje comparativo también consideró las palabras clave presentes en los documentos, sobre las cuales fueron enumerados los siguientes términos: Defensa, Seguridad, Militar, Ejército, Aeronáutica, Marina, Terrorismo, Drogas y Ciber (con sus variaciones en inglés para análisis de los documentos de Alemania y Francia). Fueron identificados, inmediatamente, la frecuencia en la cual los términos aparecen en los documentos, con el objetivo de evidenciar la preminencia de determinados asuntos en relación a los otros.

Tabla 5 - Comparación de los términos-clave

Términos clave	Defensa (Defence)	Seguridad (Security)	Militar (Military)	Ejército (Army)	Aeronáutica (Air Force)	Marina (Navy)	Terrorismo (Terrorism)	Drogas (Drugs)	Ciber (Cyber)
Alemania	53	99	49	2	0	0	13	0	28
Francia	136	136	83	2	2	4	18	2	24
Brasil	132	73	118	58	39	68	2	4	16

Fuente: Basado en France (2013), Brasil (2016) y Germany (2016).

Se percibe una mayor preminencia de la temática cibernética en relación a los temas terrorismo y drogas, temáticas tradicionales en los documentos de defensa. Ese hecho se explica por la actuación del tráfico de drogas y terrorismo a través del ciberespacio, en paralelo con las amenazas que surgen en el dominio cibernético. Todavía, el ciberespacio no es categorizado solamente como una temática de amenaza, como ocurre con los temas de terrorismo y drogas, sino como un dominio estratégico a ser titulizado y, concomitantemente, ser desarrollado desde el punto de vista económico, social, gubernamental y civil.

Es notable también el involucramiento del sector militar en el discurso brasileño, mencionando los militares y las distintas manos de las Fuerzas Armadas en una frecuencia mucho mayor que los demás países.

Desde el análisis comparado de los documentos, es posible identificar congruencias y divergencias políticas en el que se refiere la valoración estratégica del ciberespacio por naciones que están desarrollando sus políticas de defensa cibernética.

En ese sentido, es importante subrayar que de entre los países que fueron analizados, Brasil es el único que no posee documentos volcados específicamente para la ciberseguridad en el

nivel estratégico. Por más que el Libro Verde de Seguridad Cibernética de 2010 sea un documento peculiar que haya servido de base para los documentos de defensa posteriores, no fueron creados nuevos documentos que condicen con la realidad que el sector cibernético se encuentra actualmente. Mientras Alemania y Francia ya son poseedoras de documentos específicos vigentes para el sector, siendo ellos el *National Cybersecurity Strategy* (GERMANY, 2016) y el *National Cybersecurity Strategy* (FRANCE, 2015), respectivamente; en el caso brasileño, el documento que trata la cuestión cibernética es la Doctrina Militar de Defensa Cibernética (BRASIL, 2014).

6 **Conclusiones**

La recurrente preocupación con las amenazas que son oriundas de agentes estatales y no estatales, así como el reconocimiento de vulnerabilidades infraestructuras y sociales resultantes de la mayor inserción de la sociedad y consecuente dependencia del espacio cibernético, lo legitima como escenario para las relaciones de poder en la actualidad. De esa manera, el análisis de la titulización del ciberespacio en los Libros Blancos de Defensa Nacional de Brasil, Alemania y Francia auxilian en la determinación y en la comparación de estrategias de seguridad y defensa nacional.

En el momento en que el espacio cibernético es reconocido como escenario de relaciones económicas, políticas, militares y sociales, se entiende que el discurso de titulización de los Estados toma forma en sus documentos de defensa. En los documentos que fueron consultados y fueron analizados, el sector cibernético es considerado un dominio prioritario y estratégico, en el cual son definidas (aunque de manera abarcadora) las amenazas y vulnerabilidades que un Estado está sometido. Los responsables por la protección del Estado en el ciberespacio también son determinados. En lo más, la práctica de identificación de amenazas y objetivos por agentes de titulizaciones – que en este caso es el Estado – condice con el proceso de titulización que es capitaneado por la Escuela de Copenhague.

No obstante, la recurrente presencia de la cuestión del ciberespacio y su reconocimiento como dominio estratégico y prioritario de un punto de vista de defensa nacional, legitima y justifica el presente trabajo. Aunque impuestos los retos teóricos a ser considerados las peculiaridades del ciberespacio, se buscó alinear un abordaje práctico de análisis comparativo del sector cibernético en los Libros Blancos de Defensa de Alemania, Francia y Brasil. Con eso, se comprende que las perspectivas del sector cibernético brasileño todavía deben ser explotadas de manera a direccionar las directrices entre los agentes actuantes, así como ofrecer atribuciones y posibilidades de crecimiento a la seguridad cibernética en Brasil.

Referencias

AMARAL, Arthur Bernardes do. **A Guerra ao Terror e a tríplice fronteira na agenda de segurança dos Estados Unidos**. 2008. Dissertação (Mestrado em Relações Internacionais) – Pontifícia Universidade Católica do Rio de Janeiro, Rio de Janeiro, 2008.

AMORIM, Celso. Segurança Internacional: novos desafios para o Brasil. Contexto Internacional, Rio de Janeiro, v. 35, n. 1, p. 287-311, 2013.

BRASIL. Ministério da Defesa. **Livro Verde: Segurança Cibernética no Brasil**. Brasília, 2010.

BRASIL. Ministério da Defesa. **Livro Branco de Defesa Nacional**. Brasília, 2012.

BRASIL. Ministério da Defesa. **Doutrina Militar de Defesa Cibernética**. Brasília, 2014.

BRASIL. Ministério da Defesa. **Minuta do Livro Branco de Defesa Nacional**. Brasília, 2016.

BRIDI, Sônia; GREENWALD, Glenn. Documentos revelam esquema de agência dos EUA para espionar Dilma. **Fantástico,** [S.l.], 1 set. 2013. Disponible en: http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html. Accedido en: 26/11/2018.

BUZAN, Barry; WEAVER, Ole; WILDE, Jaap De. **Security:** a new framework for analysis. Boulder: Lynne Rienner Publishers, 1998.

BUZAN, Barry; HANSEN, Lene. **A evolução dos estudos de segurança internacional.** UNESP: São Paulo, 2012.

CARREIRO, Marcelo. A Guerra cibernética: cyberwarfare e a securitização da Internet. **Revista Cantareira**, Niterói, RJ, n. 17, p. 123-137, jul./dez. 2012.

CEPIK, M.; CANABARRO, D. R.; BORNE, T. A securitização do ciberespaço e o terrorismo: uma abordagem crítica. In: CEPIK, M. (Org.). Do 11 de setembro de 2001 à "Guerra Contra o Terror": reflexões sobre o terrorismo no século XXI. Brasília: Instituto de Pesquisa Econômica Aplicada, 2014. p. 161-186.

CHEN, T. **Cyberterrorism after Stuxnet**. Carlisle: United States Army War College Press, 2014.

COLLIN, B. Future of cyberterrorism: the physical and virtual worlds converge. **Crime and Justice International**, Chicago, v. 13, n. 2, p. 15-18, 1997.

DENNING, D. E. **Cyberterrorism**: testimony before the special oversight panel on terrorism. [S.l.]: Terrorism Research Center, 2000.

FARRET, Nerissa Krebs. A securitização do narcotráfico nos Estados Unidos e a influência no Brasil. **Conjuntura Global**, Curitiba, v. 3, n.2, p. 117-123, abr./jun. 2014.

FRANCE. **French White Paper on defence and national security**. Paris, 2013.

FRANCE. **National Cybersecurity Strategy. Paris**, 2015.

GERMANY. **White Paper on German Security Policy and the future of the Bundeswehr**. Berlin, 2016.

GERMANY. **National Cybersecurity Strategy.** Berlin, 2016.

GOLDANI, Carlos Alberto. **Malwares**. [S.l.]: Unicert Brasil Certificadora, abr. 2005.

HAESBAERT, Rogério. Território e multiterritorialidade: um debate. **Geographia**, Niterói, RJ, v. 9, n. 17, p. 19,46, 2007. Disponible en: http://periodicos.uff.br/geographia/article/view/13531/8731. Accedido en: 12 fev. 2018.

HILDEBRANDT, Mireille. Extraterritorial jurisdiction to enforce in cyberspace? Bodin, Schmitt, Grotius in cyberspace. **University of Toronto Law Journal**, [S.l.], v. 63, n. 2, p. 196-224, 2013.

KALLBERG, Jan; COOK, Thomas. **The unfitness of traditional military thinking in cyber**. **IEEE Access**, Piscataway, v. 5, 2017.

KENNEY, Michael. Cyber-terrorism in a post- Stuxnet world. **Orbis**, Amsterdam, v. 59, n. 1, p. 111-128, 2015.

KUEHL, Daniel T. **From cyberspace to cyberpower**: defining the problem. Washington, DC: National Defense University, 2009.

LIBICKI, Martin C. **Cyberdeterrence and cyberwar**. Santa Monica, CA: Rand Corporation, 2009.

LOBATO, Luisa Cruz; KENKEL, Kai Michael. Discourses of cyberspace securitization in Brazil and in the United States. **Revista Brasileira de Política Internacional**, Brasília, v. 58, n. 2, p. 23-43, 2015.

MOTTA, B. V. C. **Securitização e política de exceção**: o excepcionalismo internacionalista norte-americano na segunda Guerra do Iraque. 2014. Dissertação (Mestrado em Relações Internacionais) – Universidade Estadual Paulista Júlio de Mesquita Filho; Universidade Estadual de Campinas; Pontifícia Universidade Católica de São Paulo, São Paulo, 2014.

NYE, Joseph S. **O futuro do poder**. São Paulo: Benvirá, 2012.

OLIVEIRA, Marcos Aurélio Guedes de. (In)Conclusão: Sobre a Necessidade de se Pensar a Defesa a Partir do Poder Cibernético. In: MEDEIROS FILHO, Oscar; FERREIRA NETO, Walfredo Bento; GONZALES, Selma Lúcia de Moura (Org.). **Segurança e Defesa Cibernética:** da fronteira física aos muros virtuais. Recife: UFPE, 2014. p. 193-196.

OLIVEIRA, Marcos Guedes de et al. **Guia de defesa cibernética na América do Sul**. Recife: UFPE, 2017.

POLLITT, M. Cyberterrorism: fact or fancy? Computer Fraud and Security, Amsterdam, v. 1998, n. 2, p. 8-10, 1998.

PRIVACY INTERNATIONAL. London, 1 Feb. 2011. Disponible en: https://bit.ly/2WdGYIU. Accedido en: 26 out. 2018.

REEVE, Tom. France unveils cyber command in response to 'new era in warfare'. **SC Media UK**, London, Dec. 2016. Disponible en: https://scmagazineuk.com/france-unveils-cyber-command--response-new-era-warfare/article/1475678. Accedido en: 21 dez. 2018.

SAINI, Hemraj; RAO, Yerra Shankar; PANDA, Tarini Charan. Cyber-crimes and theis impacts: A review. **International Journal of Engineering Research and Applications**, Ghaziabad, v. 2, n. 2, p. 202-209, mar-abr, 2012.

SYMANTEC. **Internet security threat report**. Mountain View, CA, abr. 2016. v. 21.

TANNO, Grace. A contribuição da escola de Copenhague aos estudos de segurança internacional. **Contexto internacional**, Rio de Janeiro, v. 25, n. 1, p. 47-80, jun. 2003. Disponible en: http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-85292003000100002&lng=en&nrm=iso. Accedido en: 13 fev. 2019.

WEIMANN, Gabriel. Cyberterrorism: the sum of all fears? **Studies in Conflict and Terrorism**, Abingdon, v. 28, n. 2, p. 129-149, 2005.

WERKHÄUSER, Nina. German army launches new cyber command. DW, Bonn, 01 April 2017. Disponible en: https://p.dw.com/p/2aTfJ. Accedido en: 21 dez. 2018.

WIKILEAKS. **Espionnage Élysée**. [S.l.], 2015. Disponible en: https://wikileaks.org/nsa-france/. Accedido en: 27/10/2017

ZUCCARO, Paulo Martino.Tendência global em segurança e defesa cibernética: reflexões sobre a proteção dos interesses brasileiros no ciberespaço. *In*: BARROS, O. S. R.; GOMES, U. M.; FREITAS, W. L. (org.). **Desafios estratégicos para segurança e defesa cibernética**. Brasília: Secretaria de Assuntos Estratégicos da Presidência da República, 2011. p. 49-77.