Poder Cibernético Brasileño

Una Nueva Perspectiva en la Expresión del Poder Nacional

Mayor Luis Eduardo Pombo Celles Cordeiro, Fuerza Aérea de Brasil

Introducción

¿Cuán importante es la defensa en un país como Brasil, con escaseces en otras áreas tales como la salud, la seguridad y la educación? Esta pregunta la hemos escuchado varias veces durante los debates en los programas de los medios de comunicación, en la prensa y en artículos científicos.

La premisa de esta pregunta se basa en la ausencia de amenazas "tradicionales" externas e internas (según las definen las teorías de relaciones internacionales) que pueden afectar nuestra integridad como una nación. Esta lógica nos puede llevar a la conclusión que la defensa no debe ser una prioridad en el desarrollo de nuestras políticas nacionales y se debe considerar una cuestión de"políticas de segundo orden".

Para refutar este razonamiento, decidimos utilizar la teoría de presión lateral (Choucri, 2012), que reza que las naciones tienen una tendencia natural de extender su Influencia o territorio

para cumplir con las demandas internas de su población. Por lo tanto, para aumentar su presencia, física o de otra manera, más allá de sus fronteras, un país aplicará "presión lateral" a otro país o países a la posición deseada. Por lo tanto, concluimos que la presión lateral es parte de las relaciones internacionales entre los estados.

Por lo tanto, podemos suponer que Brasil, al igual que cualquier otro país, ejercerá presión lateral en el escenario internacional para satisfacer sus demandas internas y experimentará dicha presión por parte de otras naciones.

Este artículo se enfoca en un elemento particular de este juego que en la actualidad afecta el funcionamiento principal de nuestra sociedad: el poder cibernético. Primero, es necesario definir el poder cibernético, luego Identificar su área de Influencia en nuestra sociedad y por último proponer maneras para crear instrumentos de poder cibernético en nombre de nuestra defensa nacional.

Poder

El poder en sí es un concepto muy difícil y abstracto de explicar, aunque muchos lo han intentado. Galbraith escribió en su libro acerca del poder y concluyó que "Pocas palabras se emplean con tanta frecuencia con tan poca necesidad de reflexionar en su significado como poder, y así ha sido durante todas las edades del hombre". (John K. Galbraith, "*The Anatomy of Power*" (Anatomía del poder),1983).

Por otra parte, Max Weber, argumentó muchos años antes que el ejercicio de poder por parte del estado es sencillamente el dominio de los hombres en un puesto de autoridad que les permite imponer su voluntad sobre sus compatriotas (Weber, 2001). Analizando las relaciones entre las personas, Raffestin escribió que dondequiera que haya relaciones humanas, habrá una relación de poder porque los individuos tienen intereses divergentes (Raffestin, 1993). Por lo tanto, concluimos que la lucha por el control y poder entre dos individuos (o grupos de individuos) significa imponer nuestra voluntad sobre el otro, y esta es la noción básica al discutir las relaciones de poder.

Poder Nacional

Con el fin de discutir el parámetro del poder estatal en las relaciones internacionales, utilizamos las ideas del Manual Básico de la Escuela Superior de Guerra Brasileña (ESG) porque su punto de vista interdisciplinario y su enfoque en la defensa nacional, según se explican en el manual (ESG, 2011), ofrecen una visión adecuada del tema desde nuestro punto de vista.

Según la doctrina de la ESG, el estado debe intentar servir los deseos de la nación (los presuntos objetivos nacionales) mediante el uso de sus recursos disponibles (el poder nacional) para lograr los objetivos establecidos (a través de la política nacional) de manera que en un final la aplicación correcta del poder nacional le permitirá a la nación lograr sus objetivos nacionales según las metas establecidas por su política nacional. Así que la capacidad del estado de garantizar que se cumplan sus objetivos establecidos depende directamente de la capacidad del estado de colaborar con sus aliados internacionales y su propia población en diferentes entornos (económico, cultural, militar, social, etc.).

En la ESG se establecen dos conceptos claves: la seguridad, que es el sentido que una persona posee (y por lo tanto la sociedad en general posee) de que él o ella está protegido contra las amenazas internas y externas; y la defensa, que son las acciones que garantizan el sentido de seguridad del estado. Tal como se explica en el manual, "En conclusión seguridad es una sensación, mientras que defensa es la acción" (ESG, 2011).

Según la definición de la ESG, en la actualidad contamos con cinco expresiones de poder nacional: político, económico, científico y tecnológico, sicosocial y militar. Estas expresiones son

los instrumentos que se emplean en las actividades de defensa para proporcionar la sensación de seguridad a la nación.

El Ministerio de Defensa Brasileño afirma que para hacer el mejor uso de estas expresiones, es necesario conocer que la relación entre ellas puede variar en espacio y tiempo, según los grupos involucrados y sus intereses (MD51-M-04, 2007). En el uso de la expresión militar, en particular, esta relación entre espacio y tiempo es un factor crítico para la libertad de acción de los actores participantes y, por lo tanto, en la capacidad del estado de imponer su voluntad (MD30-M-01, 2011).

En vista de que la garantía de defensa es el producto de la noción correcta de espacio y tiempo, es importante que establezcamos la noción del tiempo (cuándo) y del espacio (dónde) que se emplean en este artículo y su relación con el poder cibernético.

Espacio y tiempo

Uno puede pensar acerca del espacio de muchas maneras. Aquí utilizaremos un concepto diferente al de la física clásica, que establece que la distancia (sinónima con el espacio) se mide en relación directa al tiempo que toma cruzarlo. Aunque también decimos que el espacio está relacionado con el tiempo que toma cruzarlo, empleamos la idea de Harvey de la "compresión de tiempo y espacio". Según su lógica, si en 1840 una carta podría viajar a una velocidad de 10 millas por hora, en 1930 su velocidad hubiese aumentado a 65 millas por hora, en 1940 a 400 millas por hora y en 1960 a 700 millas por hora (Harvey, 1989).

Si seguimos esta lógica, podemos concluir que en la actualidad el mismo mensaje está viajando a la velocidad de la luz (limitada por el sistema de transmisión) vía la *Internet*, una red externa (*extranet*) o una red interna *(intranet)*. Con base en este razonamiento y empleando como ejemplo un telegrama enviado desde São Paulo a Río de Janeiro, vemos que la distancia entre ambas ciudades (alrededor de 260 millas) no ha cambiado significativamente desde su fundación en el siglo XVI, pero los efectos del mismo mensaje se sentirán hoy más rápido que nunca antes.

Entonces lo que vemos hoy es la transformación del espacio en algo efímero, donde ir a la casa de su vecinos que está a unos pocos pies de su puerta para pedirle una taza de azúcar consumirá más tiempo que enviarle y recibir un mensaje instantáneo, una fotografía o un texto de un amigo en Beijing.

Si en el primer caso nos desplazamos a pie y en el segundo vía un mensaje en el teléfono, puede que tengamos la respuesta de nuestro amigo en China antes de nuestro encuentro con nuestro vecino. Por consiguiente, concluimos que si el sentido del *espacio* está básicamente conectado con el concepto de *tiempo*, podemos decir con certeza que el espacio no es lo mismo que distancia cuando hablamos de comunicación. Si bien la distancia es fija y se basa en la medida utilizada por el observador (metros, pies, millas, etc.), el espacio en la comunicación depende del tiempo que se requiere para que se produzca y se envíe la información desde el transmisor y la reciba e interprete el receptor, indistintamente de la distancia.

Esta comunicación rápida que vemos hoy en día crea la percepción que hemos pasado de una sociedad rígida, donde el flujo de la comunicación es restringido y rígido, a una sociedad fluida donde la información fluye entre individuos en una atmósfera de anarquía (en el sentido de *libertad o falta de control*), que ya no es gobernada por la distancia entre las partes involucradas sino por las herramientas que permiten la comunicación en tiempo real.

Este punto de vista fue propuesto por Bauman a inicios de este siglo, en un concepto que él llama "modernidad líquida". Por consiguiente, los cambios en una sociedad "fluyen" y la sociedad supone la forma del entorno que lo contiene, mientras que la sociedad anteriormente era "sólida" y requería fortaleza y presión para ser moldeada en una nueva forma (Bauman, 2001). Esta liquidez en el mundo de hoy permite cambios para penetrar todas las capas de la vida, in-

clusive la relación entre espacio y tiempo. La velocidad actual a la que la información se intercambia significa que los individuos que se comunican ya no tienen que estar presentes físicamente. Pueden estar presentes virtualmente a través de la tecnología. La "presencia" de una persona (al igual que las de otros que forman parte del círculo social, familiar o profesional de la persona) es reemplazado por el *software* en la computadora que crea a la persona virtual. En vista de que la noción entre espacio y tiempo se torna sumamente pequeña, no es necesario ir a algún lado para estar "presente", o más bien, la "presencia" ya no tiene lugar en el mundo real sino en el mundo virtual que es el concepto del "espacio viajado en un tiempo en particular" utilizado en la actualidad para la interacción entre las personas.

Por lo tanto, nos percatamos que la necesidad "real" de desplazarnos de un lugar a otro para poder interactuar (y, por lo tanto, para interactuar en una relación de poder) será reemplazada "si no completamente, al menos en parte" por la necesidad de permanecer conectados al mundo virtual. Esta necesidad influye directamente en la noción de pasado, presente y futuro en las relaciones humanas y reduce nuestra noción del espacio en un mundo donde el acceso a la información y la capacidad de comunicarnos aumenta de manera exponencial.

Todo ello es por la evolución de la tecnología (portátil o no) y su capacidad de proporcionar acceso a las redes de comunicación en las cuales un individuo puede representar sus deseos, opiniones y reclamos sin necesidad de estar atado a una representación colectiva tales como asociaciones, sindicatos, partidos políticos, ONGs y entidades similares (Choucri, 2012).

Estas herramientas de información nos permitieron, en la década de los noventa, entrar en lo que Peter Drucker llamó la era de la información. En la era de la información, las actividades se deben enfocar en la producción y diseminación del conocimiento para generar riqueza (Drucker, 1999).

Entonces, nos percatamos de la importancia de estos dispositivos que nos permiten interactuar de esta manera moderna, y es fácil comprender por qué mantenerlos conectados es importante para una sensación de seguridad, no solamente para los individuos sino para las instituciones del estado brasileño.

Por lo tanto, es necesario ofrecer la capacidad de comunicarnos con seguridad, pero sin perder los valores consagrados en nuestro contrato social: libertad de expresión, el derecho a seleccionar sus preferencias políticas y el derecho a ser dueño de propiedad y activos (ya sean reales o virtuales) y todos los demás derechos otorgados en nuestra constitución. En otras palabras, es necesario para el estado ejercer su poder nacional en este entorno virtual. Pero antes que el estado escoja cómo ejercer ese poder, primero es necesario limitar el ámbito de actuación, y en nuestra opinión esa tarea exige la creación de una nueva expresión de poder nacional: el poder cibernético.

Poder Cibernético

El término *poder cibernético* no existe, al menos no en el uso propuesto por este autor. Lo que vemos en la literatura con bastante frecuencia son las definiciones con un enfoque en la acción en el espacio cibernético, principalmente la *Internet:*

- Estrategia de seguridad cibernética: "El arte práctico de garantizar la existencia y mantenimiento de la sociedad de información en una nación, y garantizar y proteger en el espacio cibernético, sus recursos de información y estructuras críticas". (Mandarin JUNIOR, 2010).
- Guerra cibernética: "Las acciones por parte de una nación estado para penetrar las computadoras o redes de otra nación con el fin de ocasionar daños o interrupción" (Clarke and Knake, 2010).

- Poder cibernético: "La capacidad de utilizar el espacio cibernético para crear ventajas e influenciar eventos en todos los entornos operacionales y a lo largo de los instrumentos de poder"(Daniel T. Kuehl, From *Cyberspace to Cyberpower, Chapter 2* [Del espacio cibernético al poder cibernético, Capítulo 2]).
- Guerra cibernética: "Un conjunto de acciones para el uso ofensivo y defensivo de la información e información para negar, explotar, corromper y destruir los valores del opositor con base en la información, sistemas de informática y sistemas de redes de computadoras" (Ministerio de Defensa, 2007).
- Disuasión cibernética: "La capacidad en el espacio cibernético de hacerle a los demás lo que otros quisieran hacernos a nosotros". (Libicki, 2009).

El concepto que quizás se acerca más a esta propuesta puede que se encuentre en la doctrina militar de las operaciones conjuntas redactada por el Ministerio de Defensa Brasileño, donde el poder cibernético se define como "la capacidad de utilizar el espacio cibernético para crear ventajas e influenciar eventos en todos los entornos operacionales y otros instrumentos de poder".

Pero en el mismo documento, cuando buscamos la definición de espacio cibernético, encontramos que solo toma en cuenta el entorno virtual donde los datos deben ser transmitidos, procesados o almacenados (MD30-M-01, 2011). En esas definiciones, creemos que el alcance del término no incluye todos los elementos del poder cibernético en vista de que las definiciones ya no toman en cuenta al individuo ("*humanware*") o hardware, elementos claves, en nuestra opinión, para construir la idea de poder cibernético.

Por lo tanto, los conceptos enlazados en la actualidad a los asuntos de defensa y cibernéticos están en una fase pragmática, según la estructura descrita por Thomas Kuhn (Kuhn, 1991). Esto es porque no hay un consenso en cuanto a la esencia de cómo se debe analizar el asunto. ¿Se debe examinar a través de un punto de vista filosófico, cultural, militar o económico?

Entonces hoy encontramos que el estado brasileño está actuando en respuesta a situaciones que están realmente sucediendo y no planificando para el futuro a través de una planificación estratégica orientada hacia el futuro. Esto resulta en un esfuerzo capilar, con cada entidad federal afectada por esas nuevas formas de interacción tratando de cumplir sus propias necesidades.

Como un ejemplo de dicha división en las estructuras responsables de proveer seguridad en el espacio cibernético (según el concepto presentado por la ESG) en Brasil, Mandarino escribió que en el 2010, 16 —instituciones esparcidas entre agencias, departamentos y burós— fueron responsables de la seguridad cibernética del poder ejecutivo brasileño en el gobierno federal (Mandarino, 2010). Pero a nivel estratégico, donde se alcanzan los objetivos definidos por la política de seguridad cibernética brasileña, y al nivel táctico, donde las respuestas a los ataques cibernéticos se lanzan, las áreas de responsabilidad de cada una de las instituciones participantes no están bien definidas ya que no hay un nivel de autoridad más alto en la cadena de mando para el poder cibernético.

La Política de Defensa Nacional (PND), aprobada por el Decreto Núm. 5,484, del 30 de junio de 2005, fue formulada para proteger a Brasil principalmente de enemigos externos. En ella se estipulan tres campos estratégicos como prioridades: nuclear, espacial, y ciberespacial (MD, 2005).

En vista de la definición ofrecida por Nelson Jobim (El País, 2009), Ministro de Defensa desde el 2007 hasta el 2011—"contar con una buena defensa es tener la capacidad de decir no cuando uno necesita decir no"— concluimos que la independencia en las tres áreas estratégicas mencionadas anteriormente son una condición básica para proteger los intereses nacionales brasileños en el ámbito internacional, la meta principal de la PND.

En el ámbito nuclear, contamos con la Comisión Nacional de Energía Nuclear (CNEN), una agencia federal encargada de:

1. Asistir en la preparación de los programas nacionales de energía nuclear;
2. Llevar a cabo investigación, desarrollo y acciones de promoción relacionadas con el poder nuclear; y
3. Ofrecer servicios en el campo de la tecnología nuclear y sus aplicaciones para fines pacíficos y regular, otorgar licencias, autorizar, monitorear y controlar dicho uso.

La CNEN actúa tanto en el mercado civil y según las necesidades militares, por ejemplo en el proyecto brasileño del submarino nuclear (CNEN, 2014).

En el campo aeroespacial, contamos con otra agencia federal, la Agencia Espacial Brasileña (AEB), que es responsable de formular y coordinar la política espacial brasileña hacia al autonomía aeroespacial, trabajando en colaboración con socios militares y civiles (Brasil, 1994).

Sin embargo, cuando analizamos el campo de la defensa cibernética, contamos con una amplia gama de agencias involucradas pertenecientes al poder ejecutivo: el Centro para Gestión de Incidentes de Seguridad en las Redes de Computadoras, creado en el 2006 (GSI, 2006); el Centro para la Defensa Cibernética del Ejército, creado en el 2010 (EB 2010); y la oficina de Delitos Cibernéticos de la Policía Federal, creado en el 2011 (MJ, 2011), para mencionar unos cuantos.

No hay una sola agencia federal que cuente con la plena autoridad de coordinar y formular cuestiones a lo largo de todo el sector cibernético federal y la responsabilidad única y exclusiva de garantizar el uso del poder nacional en el ámbito cibernético. Por lo tanto, podemos decir que las acciones en el ámbito cibernético ahora son relegadas a actores responsables por las acciones de otras expresiones de poder nacional (como el Ejército Brasileño, que es parte de la expresión militar), pero no hay un "zar cibernético" que actúe específicamente para el poder cibernético.

Otro obstáculo es que las acciones observadas se enfocan en el uso seguro de la red global como la línea de defensa principal, y no en garantizar el acceso a las tecnologías que nos permiten tener acceso al espacio cibernético (por ejemplo, procesadores y memorias para las computadoras), que con certeza conducen a un poder nacional débil y la falta de capacidad de proveer la seguridad requerida en el campo según se estipula en la PND.

Por lo tanto, creemos que la ruptura del sistema actual es necesaria para que podamos utilizar los conceptos tratados anteriormente, no de una manera compartimentada como la de hoy en día, sino con una visión holística y deductiva del tema para poder comenzar la gestión estratégica del tema. Para que esto suceda, el primer paso es la clasificación de los asuntos que están relacionados con esta nueva expresión de poder nacional, conocido como poder cibernético, porque al hacerlo tendremos un alcance definido del entorno para comenzar nuestra planificación estratégica.

Nuestro razonamiento para la creación de una nueva expresión de poder nacional radica en el hecho de que, a diferencia de otros entornos tales como el espacio y los océanos, el espacio cibernético es un entorno creado, desarrollado, asistido y controlado por los humanos. Por lo tanto, la interacción humana es necesaria para la existencia de la cibernética. Por ende, concluimos que solo se puede tener acceso a este entorno, tan importante para la civilización, a través de los mecanismos creados por los humanos y hay pocas naciones en control de este proceso de la creación.

De manera que, si seguimos el modelo propuesto por John A. Warden III e intentamos ocasionar una parálisis estratégica por un ataque paralelo o defendernos en contra de uno (Warden, 1995), tenemos que estar conscientes que solamente prepararnos para una contienda en el espacio cibernético (considerada una red virtual como un campo de batalla) es una opinión muy limitada del problema porque de nada sirve contar con protecciones virtuales excelentes en el espacio cibernético si se nos niega la oportunidad de tener acceso al mismo. Toda nuestra planificación sería inútil.

Warden también nos enseña que en el conflicto no debemos buscar la batalla, sino, que es inteligente evitarla. Esto lo haremos buscando los centros de gravedad del enemigo, los elemen-

tos de su sociedad que afectan directamente la capacidad de combate del estado. Después de hacer esto, los atacaremos fuertemente y la lucha será breve. Por lo tanto, no debemos atacarlos individualmente, pero debemos lanzar simultáneamente ataques paralelos que culminan en la falta de capacidad del enemigo de seguir luchando y su rendición en una contienda breve pero eficaz.

Según esta lógica, mucho más eficaz que llevar a cabo ataques en la *Internet,* sería utilizar la ingeniería social para atacar el *humanware* (recursos humanos) en la expresión política de poder nacional o explotar la dependencia externa total de Brasil en el *hardware utilizado* para todas las expresiones de poder nacional de un solo golpe.

Por lo tanto, lo que proponemos como poder cibernético es un concepto que abarca no tan solo el espacio cibernético sino también la capacidad de tener acceso al mismo y a los individuos que interactúan en este entorno. Esto solamente será posible si controlamos la producción del equipo *(hardware)* y las herramientas utilizadas *(software)* y capacitamos a aquellos que trabajan con ambos elementos *(humanware).*

Considerando que en el 2010 contábamos con 16 instituciones prestándole atención a este problema, quizás algunos opinen que el problema está bien abarcado. Sin embargo, el entendimiento de este autor es todo lo contrario.

Esta conclusión se basa en algunas suposiciones. La primera es que no se ha definido un autor como el único responsable de crear la política nacional sobre la defensa cibernética con la autoridad de delegar tareas, dirigir esfuerzos y producir hojas de ruta o planes con la autoridad sobre otras organizaciones públicas y privadas. Por lo tanto, hay una falta de liderazgo al nivel más alto de decisiones en cuanto a la política nacional.

Otro problema es la falta actual de responsabilidades definidas. Por ejemplo, si un ataque cibernético afectara a la red eléctrica en una región en particular del país, ¿quién sería el responsable de los procedimientos de contención, la investigación de los infractores y, de ser necesario, la represalia? Si hablamos sobre un delito, podríamos decir que sería responsabilidad de la policía federal, pero si hablamos sobre un acto de guerra, eso sería responsabilidad del Centro de Defensa Cibernética del Ejército. Esta incertidumbre plantea otras cuestiones:

- Para un acto delictivo, ¿podemos identificar con precisión un individuo u organización como responsable?
- Para un acto delictivo, ¿qué ley aplica si el infractor llevó a cabo el acto en otro país?
- ¿Qué legitimidad tiene la Carta Brasileña de los derechos en la *Internet* en el entorno internacional?
- ¿Quién sería el responsable de negociar los términos de esa Carta de derechos en la comunidad internacional? Si clasificamos el ataque como un acto de guerra, surgirán otros problemas:
- ¿Cuáles reglas aplican en la comunidad internacional para justificar nuestro derecho a declarar la guerra (*jus ad bellum*) en respuesta a un ataque cibernético?
- ¿Bajo cuáles reglas vamos a luchar en el entorno cibernético a la vez que respetamos las convenciones internacionales (*jus in bello*)?
- En caso de un ataque cibernético oculto en un conflicto convencional, ¿quién sería el responsable de llevar a cabo las acciones (exploración, defensa y ataque) en el espacio cibernético —el Ejército Brasileño que también participaría en llevar a cabo operaciones terrestres, o una entidad que tendría la responsabilidad exclusiva del poder cibernético?

En los ejemplos anteriores, vemos solamente las implicaciones a nivel estatal, pero si pasamos al sector privado, ¿quién debe proteger las transacciones financieras, las redes de comunicaciones de datos, las redes telefónicas y la infraestructura crítica de las industrias de alta tecnología? ¿Tendría el estado esta responsabilidad y, aún más, la capacidad de extender la seguridad en estas áreas?

Estos retos no son nuevos y de hecho no son fáciles de resolver porque incluyen muchas variantes, tanto internas como externas. Como ejemplo de cómo lidiar con estos problemas, debemos analizar la obra de Harold Valadão sobre la ley aeroespacial:

A un hombre no se le entrega ningún poder nuevo sin control inmediato o legal. Es deber de la ley proteger al hombre contra los excesos de los demás hombres. Por cada progreso social, económico o tecnológico, se requiere otro tipo de cobertura legal para la persona. En el umbral de una nueva era, surge una ley nueva (1957, apud FILHO, 2007).

En cuanto a la planificación estratégica del estado con respecto a la seguridad cibernética, ¿quién responderá las siguientes preguntas?:

- ¿Es posible la independencia tecnológica en este sector?
- De no ser posible, ¿con cuáles alternativas contamos para mantener la seguridad y defensa del país?
- De ser posible, ¿cuáles sistemas y equipos diseñamos y fabricamos en el país?
- ¿Cuáles son las aptitudes que se esperan de aquellos que trabajan en la defensa cibernética?
- ¿Cuál es el papel que desempeña el gobierno, y cuál es el papel que desempeña el sector privado?

En la figura 1, vemos un ejemplo de un sistema unificado e interdependiente propuesto.

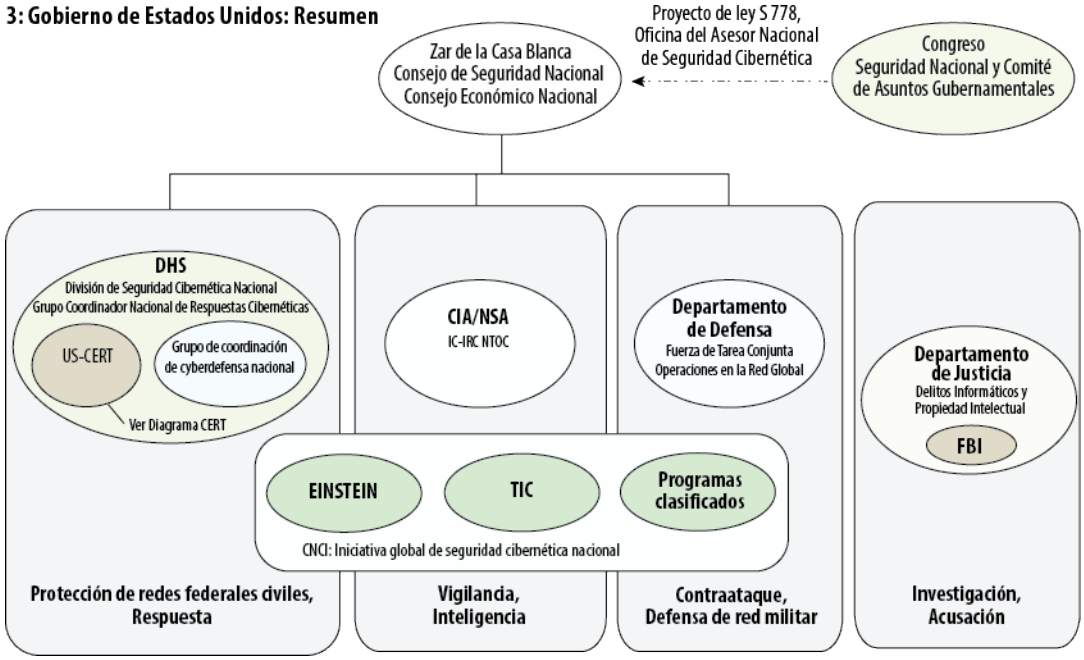

Figura 1. Estructura propuesta de la seguridad cibernética para Estados Unidos (Reimpreso de Nazli Choucri, Stuart Madnick y Jeremy Ferwerda, *"Institutions for Cyber Security: International Responses and Global Imperatives"* (Instituciones para la seguridad cibernética: Respuestas internacionales e imperativos globales), Information Technology for Development 19 (2013): 19, DOI: 10.1080/02681102.2013.836699.

Quizás esta estructura es apropiada para coordinar los esfuerzos del Departamento de Defensa de EE.UU., que define el espacio cibernético como "una estructura de red interdependiente de la tecnología de la informática y contenidos de datos, incluyendo la *Internet*, las redes

de telecomunicaciones, computadoras, comunicaciones y sistemas de informática al igual que procesadores empotrados y controles" (DOD, 2014).

En nuestra definición de poder cibernético, nosotros le agregaríamos a la definición de Estados Unidos las organizaciones que fomentan la investigación y el desarrollo al igual que la regulación de las actividades cibernéticas (inclusive la defensa) en los entornos internos y externos y en el sector privado.

Con el fin de corroborar las ideas presentadas anteriormente, este autor opina que definir un actor para que administre exclusivamente las políticas estratégicas para las operaciones cibernéticas parece ser no tan solo deseable sino también una solución inevitable. Pero antes de definir quién pagará, necesitamos definir el área de responsabilidad.

En la metodología que nosotros utilizamos, decidimos llamar esta área de actividad *poder cibernético* que es una nueva expresión de poder nacional empleando el concepto de la ESG. Creemos que esta acción ayudaría en estudios futuros creando paradigmas de manera que podamos pasar a la etapa de ciencia normal (Kuhn, 1991), donde una o más áreas podrían explorar el tema ya sea independientemente o en un enfoque interdisciplinario.

Las definiciones que utilizamos siguen a las que fueron adoptadas por la ESG:

- Hombre: El individuo o grupo de individuos con la capacidad de utilizar un dispositivo electrónico para interactuar en un entorno de red pública, privada o mixta con otros miembros de la red en una relación de poder;
- Tierra: El equipo y los sistemas operativos que le permiten al individuo o grupo de individuos interactuar en un entorno de red pública, privada o mixto con otros miembros de la red en una relación de poder; y
- Instituciones: Instituciones públicas, privadas o mixtas responsables de la sostenibilidad (en el sentido de *sustentare:* sostener, defender, apoyar, retener) de entornos de red públicas, privadas o mixtas que le permiten al *hombre* (según la definición anterior) influenciar las expresiones de poder nacional a través de la tierra (según la definición anterior).

Por último, decimos que *poder cibernético* significa la expresión de poder nacional que busca regular, controlar y desarrollar (según los principios morales de la sociedad) la transmisión de información entre individuos o grupos sociales al igual que los efectos de esta relación de poder en alcanzar y conservar los objetivos nacionales.

Conclusión

Hemos concluido que, en la sociedad de hoy, las relaciones de poder están cambiando a causa de la transformación en los conceptos de tiempo y espacio al igual que el reemplazo de presencial virtual por presencia física sin una pérdida de Influencia en las relaciones sociales.

Por las tanto, ahora las relaciones son cada vez más fluidas y adaptables al entorno en su alrededor, pero esto viene acompañado de una mayor dependencia en el acceso a equipo tecnológico ya que es la manera como disfrutamos un entorno completamente artificial creado por los humanos.

Tomando en cuenta los conceptos de la ESG, nos damos cuenta que, en el mundo actual, no podemos discutir ni la seguridad ni la defensa sin la capacidad de proyectar nuestro poder nacional en el ámbito virtual (ya sea privado o público) y que la sociedad brasileña no tendrá un sentido de seguridad si no hay confianza de que nuestra integración a la era de la informática está garantizada.

Entonces, para nosotros se nos torna necesario poder contar con la capacidad de planificar nuestra defensa en la expresión definida por nosotros como poder cibernético para poder garantizar la seguridad de nuestra nación contra un ataque cibernético concebido para ocasionar una parálisis estratégica, defendiéndonos no tan solo en el espacio cibernético sino también fuera del mismo empleando soluciones nacionales en el *hardware y el software*, por ejemplo.

Encontramos que una buena solución sería establecer una nueva expresión de poder nacional y esbozar el desarrollo de estudios, acciones y conceptos doctrinales con una visión holística de la situación. Llegamos a la conclusión que una aglutinación de esfuerzos comenzaría con la definición de todas las ideas actuales bajo un solo concepto, que llamamos poder cibernético.

Esta congregación de conceptos existentes no es una evolución de los conceptos actuales sino un cambio del sistema de reacción actual (donde esperamos que suceda un problema y luego tratamos de resolverlo).

Dicho cambio sucedería a través de la adopción de un punto de vista deductivo, contra el actual inductivo, con la asimilación de los conceptos de tiempo, espacio y relaciones de poder que son completamente diferentes de las adoptadas en la actualidad con la intención de proveer una mejor capacidad de defensa para Brasil. ❑

Referencias

Bauman, Zygmunt, Liquid Modernity (Modernidad líquida), (Rio de Janeiro: Jorge Zahar Editor .., 2001.

Comando del Ejéricto Brasileño -. EB Ordenanza Núm. 66 del 4 de agosto de 20l0.

Brasilia, disponible en:

<Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C BwQFjAA and url = http: //www.sgex.eb.mil.br/sistemas/ be / copiar.php? codarquivo ac = 824 & t = & ei = bre meLYU7DOLpLmsATi-.

YDYCA y usg = AFQjCNEmEuRHQuBtJgQJGYwSlANIM7sjNA and bvm = bv.71778758, .cWc d>. Consultado el 22 de julio de 2014.

BRASIL. Constitución Federal. Brasilia, 1988.

BRASIL Ley Núm. 8854 del 10 de febrero de 1994 Brasilia, disponible en:

<Http://www.planalto.gov.br/ccivil_03/Leis/L8854.htm>. Recuperada el 20 de julio de 2014.

Choucri, Nazli CyberPolitics in International Relations (Política cibernética en las relaciones internacionales) de Cambrida: MIT Press .. 2012.

Choucri, Nazli; Madnick, Stuart; FERWERDA, Institutional Foundations for Cyber Security (Bases institucionales para la seguridad cibernética) Jeremy: Current responses and new challenges (Respuestas actuales y nuevos retos), Accesado el 5 de julio de 2014.

CLARKE, Richard; Knake S, Robert CyberWar.'s Next threat to national security and what to do about it (La siguiente amenaza de la guerra cibernética a la seguridad nacional y qué hacer al respecto). New York: HarperCollins, 2010.

Comando del Ejército -. EB Ordenanza Núm. 666 del 4 de agosto de 2010 Brasilia, disponible en: <Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0C BwQFjAA and url = http: //www.sgex.eb.mil.br/sistemas/ be / copiar.php? codarquivo ac = 824 & t = & ei = bre meLYU7DOLpLmsATi-

YDYCA y usg = AFQjCNEmEuRHQuBtJgQJGYwSlANIM7sjNA and bvm = bv.71778758, .cWc d>. Consultado el 22 de julio de 2014.

DEPARTMENTO DE DEFENSA - DOD. DOD Dictionary of Military Terms (Diccionario de términos militares). Disponible en: <hhttp: //www.dtic.mil/doctrine/dod_dictionary/tm> Recuperado el 17 de junio de 2014.

Drucker, PF. Post-capitalist society (La sociedad postcapitalista). 7ª .ed. Río de Janeiro: Campus, 1999.

EL PAIS. "A good defense is Having the capacity To say that the that NO when is necessary say no" Madrid, 28 de octubre de 2009, disponible en: <Http://internacional.elpais.com/internacional/2009/10/28/actualidad/1256684401_8502 15.html>. Recuperado el 10 de julio de 2014.

ESCUELA SUPERIO DE GUERRA - ESG Guía Básica: Elementos Fundamentalistas I. Río, enero de 2011.

FILHO, José Monserrat The Magna Carta of outer space (La Carta Magna del espacio exterior). Disponible en: http://www.sbda.org.br/artigos/anterior/37.htm> Recuperada el 4 de julio de 2014.

Gabinete de Seguridad Institucional - GSI Ordinance No. 13, del 13 de agosto de 2006, Brasilia, disponible en: <http://www.ctir.gov.br/sobre-CTIRgov.html#quemsomos> .. Consultada el 22 de julio de 2014.

GALBRAITH, Kenneth J. Anatomy of power (Anatomía del poder) Sao Paulo: .. Pioneer, 1986.

HARVEY, David. Condition of Postmodernity (Condición de la postmodernidad). Cambridge: Blackwell Publishers, 1989.

KUHN, Thomas. S. Structure of Scientific Revolutions (Estructura de las revoluciones científicas), São Paulo Outlook 1991.

LIBICKI, Martin C .Cyberdeterrence and cyberwar (Disuasión cibernética y la guerra cibernética). Santa Monica: Rand, 2009.

MANDARIN JUNIOR, Raphael. Brazilian defense and security of cyberspace (Defensa brasileña y la seguridad del espacio cibernético). Recife: Cubzac, 2010.

MINISTERIO DE DEFENSA Armed Glossary (Glosario del Ejército) - MD35-01-G . Brasilia, 2007.

MINISTERIO DE DEFENSA. MD30-M-01 Joint Operations Doctrine first volume. (Doctrina de las operaciones conjuntas, primer volumen) Brasilia, 2011.

MINISTERIO DE DEFENSA. MD51-M-04 Military Doctrine of Defense (Doctrina militar de defensa), Brasilia, 2007.

MINISTERIO DE DEFENSA. National Defense Policy (Política nacional de defensa) Brasilia, 2005.

DEPARTMENTO DE JUSTICIA -. MJ Ordinance No. 2877, of December 30, 2011 (Ordenanza Núm. 2877 del 30 de diciembre de 2011). Brasilia, disponible en:

<Http://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CB4QFjAA and url = http: //www.dpf.gov.br/acessoainformacao/http___intranet. dpf. gov.br _legislacao_regimento_interno_portaria_n_2-877-2011-.

MJ.pdf and ei = qOTYU6LoM8bnsATIqIKACA and usg = AFQjCNG5TOa0NE6nSrVdN52c3i-cjc74XA and bvm = bv.71778758, d.cWc>. Recuperada el 24 de julio de 2014.

Comisión Nacional de Energía Nuclear - CNEN Institutional - Skills (Destrezas institucionales) disponible en: <http://www.cnen.gov.br/acnen/inf-competencias.asp>. Consultado el 15 de julio de 2014.

Raffestin, Claude. Towards a geography of power (Hacia una geografía de poder) São Paulo: Editora Attica, 1993.

VENTRE, Daniel Cyberwar and Information War (La guerra cibernética y la guerra de la informática). London: Iste 2011.

WARDENIII, John A. Enemy as a System (El enemigo como un sistema) disponible en:

<Http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm> Recuperado el 20 de junio de 2014.

WEBER, Max Science and Politics: Two Vocations (La ciencia y la política: Dos vocaciones). São Paulo: Martin Claret, 2001.

El Mayor Luis Eduardo Pombo Celles Cordeiro, Fuerza Aérea de Brasil (FABRA). Maestría, Gestión Pública; Universidad de la Fuerza Aérea, Río de Janeiro. Es responsable de la disciplina del empleo de la fuerza militar en la Escuela para Oficiales de Escuadrón de la Fuerza Aérea Brasileña en Río de Janeiro. Además, prepara los planes de estudio para los cursos y enseña la doctrina básica de la Fuerza Aérea. Antes de ocupar su puesto actual, se desempeñó en calidad de oficial de administración de personal en el 5/8 Escuadrón, Base Aérea Santa María. En calidad de egresado distinguido de la Escuela para Oficiales de Escuadrón, Base Aérea Maxwell, Alabama, el Mayor Pombo Celles es un piloto con más de 3,500 horas de vuelo en el T-25, AT-26, AT-27, C-97, C-98, U-42, H-50 H-1H y H-60L.