Revista Ensayos Militares
vol. 3 - nº 1 - 2017, pp. 77-92

ISSN 0719-6334 / versión impresa
ISSN 0719-6989 / versión en línea

Ciberdefensa, ¿hacia un nuevo eje estratégico?

Cyber Defense, Towards a New Strategic Axis?

René Leiva*
Centro de Estudios Estratégicos Academia de Guerra del Ejército de Chile

Resumen: En este artículo se sostiene que la ciberdefensa es un concepto de repercusión estratégica, con un escenario que es el ciberespacio que debe ser entendido como bien público. La ciberdefensa, además de considerarla como una nueva dimensión, se proyecta a ser un nuevo eje estratégico, lo que es coincidente con la tendencia contemporánea del actuar en el ciberespacio.

Palabras claves: Ciberdefensa – Ciberguerra – Ciberespacio

Abstract: This article argues that cyber-defense is a concept of strategic repercussion, with a scenario that is cyberspace that should be understood as a public good. The Cyber-defense, in addition to considering it as a new dimension, is projected to be a new Strategic Axis, which is coincident with the contemporary tendency of acting in cyberspace.

Key words: Cyber Defense – Cyber War – Cyber Space

Fecha de recepción: 1 de febrero de 2017
Fecha de aceptación y versión final: 22 de marzo de 2017

* René Leiva es General de Brigada (r) del Ejército de Chile. Licenciado en Ciencias Militares y Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica en la Academia de Guerra del Ejército de Chile. Diplomado de la Pontificia Universidad Católica de Chile en Gestión en Educación. Especialista en Inteligencia y Guerra Electrónica. Investigador del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. Email: rene.leiva@acague.cl leivarene@yahoo.com

"El próximo Pearl Harbor podría llegar
vía Internet"

Leon Panetta,
Ex-Secretario de Defensa de
Estados Unidos

1. Introducción

El tema cibernético se origina en la información, como elemento que ha permitido al hombre formar opiniones, comprender hechos, aclarar situaciones, de manera de darle elementos de juicio suficientes para tomar decisiones correctas. En la medida en que se fue haciendo más urgente satisfacer estas demandas, se hizo necesario disminuir los tiempos de las etapas del proceso asociado a la información, tornando evidente la necesidad de automatizar la mayor cantidad posible de procesos, dando origen a la informática.

El ciberespacio, en la definición del Departamento de Defensa de EE.UU., es el dominio global dentro del entorno de la información que consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores específicos y controladores. Se puede complementar esta definición con lo que conceptualiza la Comisión Europea como "el espacio virtual por donde circulan los datos electrónicos de los ordenadores del mundo" y por último la UIT (Unión Internacional de las Telecomunicaciones) como el lugar creado por medio de la interconexión de sistemas de ordenador mediante Internet.[1] Entonces el ciberespacio existe en lo virtual, con efectos en lo real, conformando un escenario creado y sustentado, con una intangibilidad en su concreción, pero con un claro impacto cuando es afectado.

Desde el nacimiento de la cibernética, en enero de 1948, pasos gigantes se fueron dando para el mejoramiento de las capacidades de procesos, tanto como la amplitud de las aplicaciones desarrolladas. Por lo mismo, los requerimientos de velocidad y memoria fueron en rápido ascenso, demandando mucho mayores avances tecnológicos. Rapidez y memoria eran los factores iniciales de cada "armatoste cibernético", caracterizados en sus inicios por sus grandes dimensiones volumétricas y consumos de energía. Fue impulsada inicialmente por Norbert Wiener con el objeto "del control y comunicación en el animal y en la máquina" o "desarrollar un lenguaje

[1] Joaquín Ruiz Díaz, "Ciberamenazas: ¿El terrorismo del Futuro?", en *IEEE.ES*, Documento de Opinión 86/2016.

y técnicas que permitieran abordar el problema del control y la comunicación en general".

2. Aparece la ciberguerra

La conformación de grandes bases de datos aisladas desconectadas unas de otras, contenidas en un computador aislado de su entorno, acumulando enormes cantidades de datos que no podían salir de él, pasó a constituir un problema tecnológico que había que solucionar, por lo que la aparición en enero de 1983 de ARPANET y el protocolo TCP/IP vino a abrir los ojos respecto de que los próximos desafíos, más que por la capacidad de proceso y almacenamiento, marcharían decididamente a lograr mayor y mejor conectividad.

Por ello en el pasado los sistemas informáticos eran relativamente seguros por encontrarse conectados a una reducida cantidad de subsistemas externos y por constituir elementos de gran valor monetario y dimensión volumétrica, lo que los hacía escasos. Hoy lo que los ha hecho vulnerables es la reducción de sus tamaños y costos, junto con ser diseñados como dispositivos de arquitecturas abiertas y con amplia conectividad a sistemas locales, regionales e incluso internacionales, de transferencia de información de gran velocidad y compleja identificación de su punto de origen. Por esta razón, se ha experimentado una disminución en los niveles de seguridad informática que presenciamos en los inicios de la informática.[2]

IBM 1401, el primer computador digital que llegó a Chile, en 1961.

[2] Martin Libicki, "The future of information Security", en *Institute for National Strategic Studies*, mayo de 2000, p. 1.

En esta necesidad de conectividad aparece la ciberguerra como un elemento nuevo, una amenaza que modifica un segmento virtual del planeta que se interrelacionaba sin mayores regulaciones, pero que con esta nueva amenaza comienza a adoptar medidas de índole defensivo y ofensivo.

Al analizar la historia de la guerra,[3] Boyd[4] vio que la victoria constantemente recaía en el lado que podía pensar con más creatividad (orientarse a sí mismo) y luego actuar rápidamente sobre tal entendimiento. Por ello, debido al hincapié en la fase de orientación del circuito que manifiesta la teoría del OODA Loop, en términos prácticos es posible establecer que cualquier crisis debería considerar una estrategia dirigida a afectar el pensamiento del liderazgo enemigo. De esta forma, la guerra de la información se ha convertido en una herramienta cada vez más relevante en el desarrollo y consecución de las crisis modernas entre Estados, toda vez que existe un gran nivel de acceso y dependencia de las tecnologías de la información y comunicaciones (TIC) de la sociedad y sus instituciones, para un correcto y oportuno proceso de toma de decisiones. Como resultado de esto, el gran nivel de intercambio de información que caracteriza a una sociedad globalizada, se ha convertido tanto en una fortaleza como en una vulnerabilidad de los países modernos. Así, el conocimiento le otorga poder a quien lo posea. Por ello quien controle el flujo de información posee ventaja, propendiendo de esta forma a obtener "información perfecta para uno mismo e ignorancia impuesta para el enemigo, ya sea por medio de la negación o la manipulación". Es en el ámbito de esta esfera de información donde se constituye un centro de gravedad potencial y relevante, con efectos de la ciberguerra.

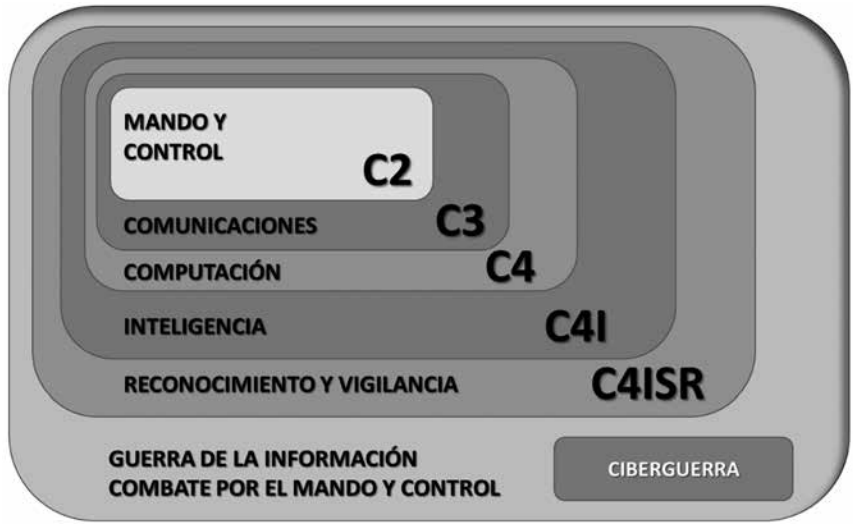
Lo que hace complejo de manejar el tema de la ciberguerra es que no corresponde a un término plenamente conceptualizado doctrinariamente, pero es un concepto que en lo militar obedece a una parte de la guerra de la información, cuya operacionalización responde al combate por el comando y control, bajo el englobamiento de la infoguerra.

Es en este combate por el comando y control donde puede entenderse que tiene cabida la aplicación militar de la ciberguerra, generando nuevas amenazas y herramientas para accionar en el campo de batalla moderno, con un efecto que puede ser transversal a todas sus dimensiones (aire, mar, tierra, espacio).

---

3 Luis Sáez Collantes, *La Ciberguerra en los Conflictos Modernos*, FACH, 2012.

4 John Boid, *The School of Advanced Airpower Studies. The Paths of Heaven: The Evolution of Airpower Theory*, Alabama, USA: Air University Press, Maxwell Air Force Base, 1997, p. 357.



Fuente: Elaboración propia, basado en el Manual "Information Operations, FM34-1".

Aporta a este encuadramiento conceptual el conjunto de esfuerzos realizados a nivel civil por el Department of Homeland Security (DHS) de EE.UU. y otros organismos, complementado con el desarrollo de las capacidades de Ciberdefensa llevado a cabo por el Departamento de Defensa (DoD), que incluye la Ciberdefensa o Ciberguerra dentro del concepto más amplio de "Guerra de la Información", que en la actualidad se denomina "Operaciones de Información" ("Information Operations, IO").[5]

Ciertamente, como todo recurso bélico disponible, presenta dos grandes líneas de aplicación: una defensiva que busca la protección de los propios medios a la acción de la ciberguerra que pueda desarrollar el adversario, y otra ofensiva con la intención de afectar al potencial enemigo.

La ciberguerra es una acción que permite su empleo desde distancias remotas, con una identificación dificultosa de quien la origina, que busca un accionar oculto o clandestino.

En esta ciberguerra se busca irrumpir o destruir los sistemas de comunicación e información del adversario, junto con tratar de obtener el máximo de información del enemigo mientras se le niega el acceso a la propia. Implica tornar el "balance de información y conocimiento" a favor propio, para así emplear el conocimiento útil

[5] Pastor Acosta, Pérez Rodríguez y otros, *Seguridad Nacional y Ciberdefensa*, ISDEFE-UPM, Cuadernos Cátedra nº 6.

obtenido en beneficio de la economía de la fuerza y la reunión de los medios. Esta forma de combatir implicará diversas tecnologías, medios de mando y control, de obtención, proceso y difusión de inteligencia, de comunicaciones, de armas inteligentes, cegamiento electrónico, perturbación (*jamming*), decepción, intrusión en los sistemas de información y comunicaciones adversarios, entre otros.

La ciberguerra adquiere su importancia al concretar una extensión de la forma tradicional de obtener información en tiempo de guerra, es decir, mediante un nivel superior de mando, control, comunicaciones e inteligencia, junto con buscar identificar, localizar, sorprender y engañar al enemigo antes de que él haga lo mismo contra nosotros.[6]

La ciberguerra presenta la característica que corresponde a una acción que rompe la clásica delimitación entre combatientes militares y civiles, ya que un alto porcentaje de comunicaciones militares en lo estratégico son canalizadas por sistemas de propiedad de civiles o que son operados por ellos. Luego, un ciberataque puede ser conducido o ejecutado tanto por civiles como por militares sobre blancos tan sensibles como sistemas de interconexión eléctrica, de transporte, infraestructuras de comunicaciones o financieras, etc., objetivos que pueden escapar a la clasificación de ser netamente militares, afectando por igual a combatientes y no combatientes.[7] En ello identificamos blancos de infraestructura crítica, con efluvios de guerra total, al cubrir todos los ámbitos de acción, afectando la población civil y los servicios que requiere para subsistir.

La aplicación de la ciberguerra más que estar orientado al envío de mensajes electrónicos o *e-mails* vía internet o afectar bases de datos de información o transferencia, lo que es más propio de los denominados *hackers*, busca una connotación superior al identificar sus objetivos en la neutralización o bloqueo de infraestructura crítica. Es una combinación de los conceptos de guerra y ciberespacio, que designa al conflicto militar en función de los medios de la tecnología de la información que utiliza en pro de la consecución de sus fines, destacándose que la velocidad de los cambios que permite el ciberespacio implica que se requiere de poco tiempo para realizar un ataque o para implementar nuevas defensas, comparado con lo que sucede en el espacio físico, respecto de operaciones convencionales durante conflictos armados tradicionales.

---

6 John Arquilla, Cyberwar *and Netwar: New Modes, Old Concepts, of Conflict, Cyber War is Coming*, Comparative Strategy, vol. 12, RAND's home page, pp. 141-165.

7 Gregory Walters, *A New way of War* in *the Information Age, The Community of Rights in an Information Age*, Centre de Recherche et D'Enseignement, Universsité d'Otawa, mayo 2000, p. 3.

Al conformar una visión de las ciberamenazas se debe tener cuidado en no caer en el sesgo de analizarlo como un factor que requiere solo la atención de las entidades policiales como parte de la protección de plataformas complementarias que pueda usar el terrorismo, ya que eso sería tener un reducido y focalizado espectro del amplio campo en que este factor puede incidir.

3. El ciberespacio como quinto dominio

El ciberespacio es considerado como el Quinto Dominio, junto con lo terrestre, marítimo, aéreo y el espacio, por esta razón, debe existir especial preocupación con el concepto de ciberguerra, que en sí no es un fin, pero puede constituir una buena herramienta como estrategia de acción.[8] Ejemplos de sabotaje de Israel a la capacidad nuclear de Irak, espionaje de países orientales a otras potencias, son presentados como recursos usando medios que operan sobre la plataforma de ciberguerra.

Fuente: May. Alejandro Gómez Abutridy.

Las nuevas tendencias muestran al ciberespacio como un elemento de poder dentro de la seguridad nacional y es mediante este nuevo y artificial dominio que se ejerce una innovadora influencia estratégica en el siglo XXI. Acá hay presencia de un ícono estratégico, en un mundo virtual donde hasta los actores más modestos

[8] Alejandro Amigo Tossi, *Ciberdefensa en las Operaciones Militares*, Seminario ACAPOMIL, Tendencias Tecnológicas Asociadas a la Ciberdefensa, agosto 2016.

pueden ser una amenaza para las grandes potencias, forjándose y desarrollándose el concepto de las operaciones militares centradas en redes.[9] En los conflictos tradicionales existen fronteras y límites, mientras que en el ciberespacio no. Para realizar un ciberataque no es necesario desplazarse, moverse o tener que pasar una frontera. Esta es una de las principales características de este tipo de fenómeno. El ciberespacio es un ambiente único, sin fronteras geográficas, anónimo, asimétrico y puede ser fácilmente clandestino.[10]

En una visión geoestratégica, el territorio se ha convertido en uno de los elementos constitutivos del Estado, por lo que su ocupación y defensa constituyen objetivos necesarios para la propia continuidad histórica del Estado.[11]

Por lo que se refiere a la ocupación del territorio adquiere dos formas complementarias entre sí: la ocupación física y la ocupación funcional.[12] La primera se inicia con el acceso de las colectividades humanas a un determinado territorio y su asentamiento de forma permanente en el mismo. Ello implica delimitar su área de ocupación respecto de la de otros Estados mediante la fijación de unas fronteras (terrestres, aéreas y, en su caso, marítimas) que se deben controlar y defender de manera permanente como requisito necesario para garantizar su seguridad. Esto tiene una extensión en su aplicación a los espacios, que siendo de la jurisdicción del Estado-nación, trascienden de lo físico y subsisten en lo virtual, donde claramente el ciberespacio tiene cabida como territorio virtual, por tanto debe ser controlado y defendido.

En segundo lugar la sociedad debe ejercer el derecho de propiedad y explotación de todos los recursos existentes en el territorio nacional para garantizar su supervivencia y desarrollo. En ello se identifica una ocupación funcional y el territorio virtual del ciberespacio debe ser asegurado en su derecho de propiedad y uso, como parte de esa ocupación funcional. No hacerlo sería desproteger un bien público y sería una desatención del Estado, en su rol de seguridad y defensa.

Respecto de la estrategia típica de un ciberataque, la mayoría de las intrusiones aprovechan las vulnerabilidades de los sistemas informáticos, particularmente de las redes críticas, donde el alcance, dirección, duración y propósito de los ataques cibernéticos observados son difíciles de identificar, ya que a menudo resulta complejo detectar y diferenciar los hilos de las diversas relaciones de causa y efecto que los caracterizan. En tal sentido, un adversario puede emplear diversas técnicas de

---

9 Vicente Adrianna Llongueras, *La Ciberguerra; la guerra inexistente*, Tesina Doctorado en Paz y Seguridad Internacional, Instituto Universitario General Gutiérrez Mellado, 2011.

10 Pastor Acosta, Pérez Rodríguez y otros, ISDEFE-UPM, op. cit.

11 Rafael Calduch Cervera, *La* Ocupación *del Territorio Nacional y la Disuasión para su Defensa: La Cambiante Perspectiva Europea*, Universidad Complutense de Madrid.

12 Ibidem.

encubrimiento para ocultar el origen de la acción, lo que complica su trazabilidad. Por ello, la determinación de la autoría, es decir, la identificación y localización de un atacante para iniciar las contramedidas, es un objetivo relevante y prioritario, pero sin lugar a dudas difícil de lograr.[13]

El concepto de defensa dice relación con la acción y efecto de conservar la posesión de un bien o de mantener un grado suficiente de libertad de acción para alcanzar tal bien. La defensa nacional es el conjunto de medios materiales, humanos y morales que una nación puede oponer a las amenazas de un adversario en contra de sus intereses.[14] Luego, la orientación de empleo de medios para la conformación de una capacidad de ciberdefensa debe ir necesariamente asociado a lo que el concepto de defensa nacional impone, es decir, la consecución de un grado de libertad de acción en el uso del ciberespacio, como también una capacidad de oposición a la ciberamenaza.

En un paso previo a visualizar algunos esbozos de enfrentamiento o mitigación a la amenaza, se hace necesario ahora conceptualizar la ciberdefensa y la ciberseguridad, que muchas veces son confundidos, pero que tienen segmentos de interpenetración, lo que tiene impacto en sus jurisdicciones, estructuras, potencialidades y rangos de acción.

La ciberdefensa[15] es una connotación sistémica y sistemática que deben desarrollar los gobiernos para comprender sus responsabilidades de Estado, en el contexto de un ciudadano y las fronteras nacionales electrónicas o digitales. Un concepto estratégico de los gobiernos que requiere la comprensión de variables como las vulnerabilidades en la infraestructura crítica de una nación; las garantías y derechos de los ciudadanos en el mundo *online*; la renovación de la administración de justicia en el entorno digital; y, la evolución de la inseguridad de la información en el contexto tecnológico y operacional. En pocas palabras, es la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional.[16]

Además, el concepto de ciberseguridad es definida[17] como "El conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para

---

13 Saez Collantes, op. cit.

14 *Libro de la* Defensa *Nacional*, MDN, Chile, Parte 2, Ed. 2010, p. 80.

15 Jeimy J. Cano, *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global,* Sistemas (Asociación Colombiana de Ingenieros de Sistemas). vol. 000, nº 0119 (abr-jun. 2011), pp. 4-7.

16 Lineamientos de Política para ciberseguridad y ciberdefensa, Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación.

17 Unión Internacional de Telecomunicaciones, referida en Alejandro Gómez Abutridy, "Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra", *Memorial del Ejército de Chile*, nº 492, agosto 2014.

proteger los activos de una organización y a los usuarios en el ciberentorno". Como realidad complementaria de la ciberdefensa, esta contribuye a la defensa digital como parte del interés nacional, en un conjunto de variables claves, en donde es necesario el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad, en el contexto de una realidad digital y de información instantánea.

La UIT[18] (Unión Internacional de Telecomunicaciones), entendiendo que la problemática de la ciberseguridad requiere un esfuerzo colectivo y coordinado entre los diferentes países, establece cinco elementos fundamentales para desarrollar una estrategia de ciberseguridad, acorde con la realidad de cada una de las naciones: desarrollo de un marco legal para la acción, desarrollo y aplicación de medidas técnicas y procedimentales, diseño y aplicación de estructuras organizacionales requeridas, desarrollo y aplicación de una cultura de ciberseguridad y la cooperación internacional.[19]

La ciberseguridad consta de tres elementos fundamentales que forman parte de los objetivos que intentan afectar los potenciales atacantes. Estos son la confidencialidad, la integridad y la disponibilidad de los recursos, CIA (Confidentiality-Integrity-Availability).

Fuente: Elaboración propia.

---

18 UIT es el principal organismo de las Naciones Unidas para la sociedad de la información y temas relativos a la tecnología de las comunicaciones. Su misión de llevar los beneficios de las TIC a todos los habitantes del mundo consiste en permitir el crecimiento y el desarrollo sostenible de las redes de telecomunicaciones y de información; facilitar el acceso universal para que todos en todas partes puedan participar en la economía y la sociedad mundial de la información y beneficiarse de ellas movilizando los recursos técnicos, financieros y humanos necesarios para concretizar esta visión. Fuente: www.onu.cl

19 Cano, op. cit.

En consecuencia, la ciberseguridad puede ser definida como la capacidad del Estado para minimizar el nivel de riesgo al que están expuestos sus ciudadanos, ante amenazas o incidentes de naturaleza cibernética.[20]

Por ello, en el ámbito estratégico, surge la pregunta de cómo generar disuasión en una quinta dimensión, en el ciberespacio, donde la sorpresa y el secreto son claves, pero donde la necesidad de exteriorizar esa capacidad debe darse.

El Libro de la Defensa de Chile nos orienta a esa respuesta, al señalarnos que el concepto rector de la estrategia de seguridad nacional de Chile es el de intentar obtener los objetivos nacionales pacíficamente por medio de la cooperación, la negociación y el acuerdo con otros Estados, neutralizando las amenazas por la vía de la disuasión y enfrentándolas militarmente solo si ella no produjera los efectos deseados. Por ello, dentro de los descriptores o guías estratégicas generales que van conformando la Política de Defensa aparece: "La disuasión más eficaz es aquella que insinúa la potencial capacidad de vencer. Es decir, la mejor forma de disuadir es preparándose para vencer".[21] Se destaca en ello el "insinuar el potencial", porque en este punto estará la capacidad de disuasión de la ciberdefensa para con las acciones agresivas que puedan potencialmente existir y a las que debe generar protección. La ciberdefensa en ello deberá contar con una capacidad de monitoreo de normalidad, cambios y alteraciones; de alistamiento constante de su batería de respuestas eficaces, debidamente planificada, coordinada y ensayada; desarrollar un grado de resiliencia de los sistemas; proveer inteligencia cibernética y rápida respuesta ciberforense. El mensaje a dar, en lo disuasivo, es que estaré vigilante, con capacidad de impedir tempranamente o al menos mitigar efectos de ciberagresión, pero junto con ello, que tendré la capacidad de saber de dónde provino ese ataque.

Pero la ciberdefensa también debe contar con un vector ofensivo. Si consideramos que la guerra se gana poniendo al enemigo en una situación en que acceder a lo que se le está requiriendo sea menos malo para él que resistir a ello, y la forma de ponerlo en esta situación es mediante una combinación de acciones militares, económicas, diplomáticas y psicológicas que lo lleven a una o más de las siguientes condiciones: La destrucción de sus fuerzas militares; la conquista y ocupación de su territorio; el quiebre de la voluntad de lucha de su ejército, de su gobierno, de su opinión pública, o de todos ellos,[22] son todos factores en que el ariete ofensivo de la ciberdefensa ciertamente va a aportar.

---

20 Consejo Nacional de Política Económica y Social Colombia, op. cit.

21 Fernando Thauby García, "Disuasión y Defensa", *Revista de Marina*, Armada de Chile, 1992.

22 Thauby, op. cit.

Ese plan de acción debe ser coherente y creíble para así generar disuasión. Esta capacidad de actuar por el disuasor posee una limitación clara en los requisitos de la proporcionalidad y la coherencia. El primero exige una proporcionalidad entre la conducta que se desea inducir en el actor disuadido y los efectos del uso del poder coactivo con el que se le amenaza. Precisamente este criterio de la proporcionalidad de la disuasión exige que esta sea graduable, es decir, que la amenaza del poder coactivo pueda incrementarse o reducirse en correspondencia con la conducta que siga la parte disuadida.[23]

A mejor entendimiento de la amplitud del escenario a cubrir, se trae a la vista parte de la Política Nacional de Ciberseguridad de Chile,[24] que define que la infraestructura de la información de los siguientes sectores será considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras. Complementa lo anterior la lectura de la Estrategia Nacional de Seguridad de Reino Unido del año 2010.[25] En ella se incluye como aspecto prioritario la protección de las infraestructuras críticas del país, y se determina que Internet es parte de estas infraestructuras, y que puede ser tanto un objetivo como un medio para terroristas, criminales y naciones hostiles.

Es tanto el impacto y la necesidad de coordinación transversal en todos los campos de acción, que la ciberdefensa requiere ser considerada como un nuevo eje estratégico en la Política de Defensa.

La respuesta para ello contemplada en el *Libro Blanco de la Defensa* de Francia 2013,[26] plantea un concepto altamente interesante y que encaja de manera plena dentro de lo que son actividades propias de ciberdefensa. La visión gala considera una postura estratégica para determinar el origen de los ataques, organizar la resiliencia de la Nación y responder a ellos, también mediante una respuesta agresiva, denominada "Lucha Informática Ofensiva" (LIO), y que parte del principio que para saber defenderse es necesario también saber atacar. Para poder lograr esta capacidad se debe invertir en los siguientes ejes principales:

– Definición de un marco de uso que cubra específicamente el conjunto de acciones relevantes de la lucha informática.

---

23 Calduch, op. cit.

24 Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022.

25 A Strong Britain in an Age of Uncertainty: The National Security Strategy, Reino Unido, © Crown Copyright, 2010.

26 *Le Livre blanc sur la défense et la sécurité nationale*, Ministerio de Defensa de Francia, Ed., 2013.

– El desarrollo de herramientas especializadas (laboratorios técnico-operativos, redes de ataque, etc.).
– La formulación de una doctrina de empleo de las capacidades de "Lucha Informática Ofensiva" (LIO), considerando planificación, realización y evaluación de las operaciones.
– Puesta en marcha de una formación adaptada, y regularmente actualizada, para personal identificado y reunido, dentro de células de especialistas.

Fuente: Elaboración propia, basado en los sitios *web* de los respectivos Ministerios de Defensa.

En el contexto regional[27] se puede apreciar claramente un mayor entendimiento y compromiso por el diseño y concreción de un grado de protección de la infraestructura, redes estratégicas, información electrónica y el fortalecimiento de organismos interinstitucionales para hacer frente a las amenazas que atentan a la seguridad del Estado, llegando a constituir el concepto estratégico que la ciberdefensa debe ser entendido como bien público.

Las ideas van desde lo meramente conceptual como es tener un estándar básico compartido en el diseño y seguridad de las redes, hasta implementación de instalaciones que cooperan y monitorean activamente las redes informáticas, con el objetivo de generar seguridad, protección y hasta capacidad ofensiva en la línea cibernética.

También ya se ha marcado la tendencia de separar aguas en lo que corresponde a la ciberseguridad y la ciberdefensa, misiones que les son propias, estableciendo actores específicos y dedicados a cada ámbito y ministerios con jurisdicción sobre cada uno de ellos, donde los requerimientos operacionales han tenido una mirada integral y multidisciplinaria, con atención puesta en las nuevas tecnologías, capacitación y

[27] Observatorio, CEE AG, septiembre, 2016.

preparación de personal técnico, como también la participación necesaria junto con el sector defensa (con visión conjunta), empresarial y académico para obtener resultados más eficientes y productivos.

UNASUR también ha continuado en el desarrollado de iniciativas en el ámbito de la ciberdefensa, manteniendo esfuerzos consignados en su Plan de Acción 2016 y tiene previsto junto con el Consejo Suramericano de Infraestructura y Planeamiento de UNASUR (COSIPLAN), la realización de un Seminario acerca de esta temática, bajo la responsabilidad directa o asociada de Chile, Ecuador, Perú, Argentina, Bolivia, Brasil y Uruguay.

4. Conclusiones

La tendencia futura se puede visualizar como orientada a iniciativas que se asocien a medidas de confianza mutua, donde se puedan compartir estructuras organizacionales superiores, marcos jurídicos o regulatorios, evaluaciones de riesgos y amenazas locales o que puedan escalar e impactar a lo regional, contando además con una visión respecto de las tendencias globales y sus efectos.

El desafío es buscar la consolidación de una línea de acción de seguridad y defensa, con presencia en lo militar y en lo civil, regulada e integrada como ámbito de la defensa nacional, con capacidades para realizar operaciones de prevención de conflictos y gestión de crisis. En ello, la construcción de una arquitectura de diseño y protección de la plataforma de ciberespacio, donde todos los estamentos de gobierno, militares, civiles, académicos y privados estén invitados a colaborar, resultará sustancial.

Se cierra entonces con el concepto que la ciberdefensa es entendido como bien público, que debe ser presentada como un nuevo Eje Estratégico, además de entenderla como una nueva dimensión, donde se debe potenciar este factor como capacidad estratégica, lo que es coincidente con la tendencia contemporánea del actuar en el ciberespacio.

Bibliografía

A Strong Britain in an Age of Uncertainty: The National Security Strategy, Reino Unido, 2010.

Acosta, Pastor, Pérez Rodríguez y otros, *Seguridad Nacional y Ciberdefensa*, ISDEFE-UPM, Cuadernos Cátedra nº 6.

Adrianna Llongueras, Vicente, *La Ciberguerra; la guerra inexistente*, Tesina Doctorado en Paz y Seguridad Internacional, Instituto Universitario General Gutiérrez Mellado, 2011.

Amigo Tossi, Alejandro, Ciberdefensa en las Operaciones Militares, Seminario ACAPOMIL, Tendencias Tecnológicas Asociadas a la Ciberdefensa, agosto 2016.

Arquilla, John, *Cyberwar and Netwar: New Modes, Old Concepts, of Conflict, Cyber War is Coming, Comparative Strategy*, vol. 12, RAND's home page.

Boid, John, *The School of Advanced Airpower Studies. The Paths of Heaven: The Evolution of Airpower Theory*, Alabama, USA: Air University Press, Maxwell Air Force Base, 1997.

Calduch Cervera, Rafael, *La Ocupación del Territorio Nacional y la Disuasión para su Defensa: La Cambiante Perspectiva Europea*, Universidad Complutense de Madrid.

Cano, Jeimy J. , *Ciberseguridad y ciberdefensa: dos tendencias emergentes en un contexto global*, Sistemas (Asociación Colombiana de Ingenieros de Sistemas). vol. 000, nº 0119 (abr-jun. 2011).

Ejército de EE.UU., Information Operations, FM34-1.

Koch, Sebastián, "La política de ciberdefensa en Chile", Columna de Opinión, http://www.losriosaldia.cl/?p=19065

Le Livre blanc sur la défense et la sécurité nationale, Ministerio de Defensa de Francia, Ed., 2013.

Libicki, Martin, "The future of information Security", en *Institute for National Strategic Studies*, mayo de 2000.

Libro de la Defensa Nacional, MDN, Chile, Parte 2, Ed. 2010.

Lineamientos de Política para ciberseguridad y ciberdefensa, Consejo Nacional de Política Económica y Social, República de Colombia, Departamento Nacional de Planeación.

Observatorio, CEEAG, septiembre, 2016.

Propuesta de Política Nacional de Ciberseguridad (PNCS) 2016-2022.

Ruiz Díaz, Joaquín, "Ciberamenazas: ¿El terrorismo del Futuro?", en *IEEE.ES*, Documento de Opinión 86/2016.

Saez Collantes, Luis, *La Ciberguerra en los Conflictos Modernos*, FACH, 2012.

Thauby García, Fernando, "Disuasión y Defensa", *Revista de Marina*, Armada de Chile, 1992.

Unión Internacional de Telecomunicaciones, referida en Alejandro Gómez Abutridy, "Ciberseguridad y Ciberdefensa, Dos elementos de la Ciberguerra", *Memorial del Ejército de Chile*, nº 492, agosto 2014.

Walters, Gregory, *A New way of War in the Information Age, The Community of Rights in an Information Age*, Centre de Recherche et D'Enseignement, Universsité d'Otawa, mayo 2000.