CAPÍTULO 5

Efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica

*Carl Marowski Pilowsky**

Introducción

La infraestructura crítica de una nación puede estar sujeta de ataques cibernéticos por parte de grupos internacionales o de individuos provenientes desde otro Estado o desde el interior de la propia nación. Estas situaciones, normalmente repentinas o no previstas, pueden generar múltiples escenarios de riesgo que configuran una verdadera amenaza para la estructura nacional de carácter sensible, considerando la correspondiente a la Defensa Nacional, a la de sus instituciones y, también, la perteneciente a las organizaciones que las apoyan y contribuyen a su sostenimiento.

Estos riesgos y amenazas pueden circunscribirse en sectores públicos o en organizaciones privadas que tengan repercusiones en el sector defensa, sea durante tiempos de paz, crisis o de guerra. Es por ello que los ciberataques pueden ser dirigidos a las estructuras de los organismos superiores de la defensa de un país, afectando la operacionalidad de los niveles estratégicos y operacionales de los estados mayores conjuntos, o interrumpiendo la conducción militar hacia los objetivos tácticos, en donde los sistemas de

* Carl Marowski Pilowsky es Coronel (R) del Ejército de Chile, Magíster en Ciencias Militares con mención en Gestión y Planificación Estratégica y (C) para la mención en Disuasión y Defensa, Magíster en Ciencias Marítimas con mención en Estrategia, Oficial de Estado Mayor en el Ejército de Chile y en la Armada de Chile, Profesor de Academia en Historia Militar y Estrategia y en Organización y Personal. Diplomado en Políticas Públicas por la Universidad Adolfo Ibáñez de Chile. Experto en Operaciones de Paz y en Derecho Internacional Humanitario con numerosos cursos internacionales en estos ámbitos de la seguridad internacional. cmarowskip@acague.cl.

mando y control se transformarán en los principales objetivos del adversario, ya sea en los planos terrestres, marítimos, aéreos, espaciales o en aquellos virtuales del ciberespacio, como también, hacia cualquier otro sector estatal, semiprivado o privado, de la banca, comercio, prensa, industria o cualquier otro sector componente o área específica, de la denominada infraestructura crítica nacional.

De la reflexión anterior se desprende la siguiente pregunta que orientará la investigación: ¿cuáles son los efectos de los riesgos y amenazas de la ciberguerra en la infraestructura crítica? Para responder esta interrogante primero se identifican los riesgos y amenazas que pueden afectar la infraestructura nacional, especialmente la relacionada con la defensa. A continuación se analiza la infraestructura crítica en el contexto de la ciberguerra. Posteriormente se analizan los efectos de la ciberguerra en la infraestructura crítica; y, finalmente, se presentan reflexiones finales que sintetizan una respuesta a la interrogante de investigación planteada.

Lo anterior se realiza revisando experiencias o tendencias que contribuyen a anticipar, detectar, precaver e identificar los principales riesgos y amenazas a los sistemas de mando y control y sus consecuentes efectos en las operaciones militares.

Los riesgos y amenazas en la infraestructura crítica

Desde lo académico, la seguridad de un Estado se identifica como el producto del conjunto de actividades que se realizan para el logro de los objetivos y, simultáneamente, para resguardar los intereses nacionales en relación con los riesgos, amenazas e interferencias importantes provenientes del entorno cercano o lejano. En este sentido, la seguridad consiste en una condición que se desea establecer para que se realicen en total normalidad todos los fines del Estado, particularmente los de desarrollo social y económico que apuntan al bienestar y el bien común de toda la población. De igual forma, para conceptualizar adecuadamente los riesgos y amenazas de una nación, es necesario mencionar la existencia de los denominados “problemas de la seguridad actuales”, los que se pueden definir, entre otras visiones existentes, como amenazas, amenazas emergentes y amenazas tradicionales.

Resulta interesante lo que la Organización de Estados Americanos (OEA) sostiene respecto de los denominados “problemas intersectoriales”¹, porque

¹ Organización de los Estados de América (OEA), Declaración de Seguridad de las Américas, 2003, p. 4.

allí se establece que ellos afectan al desarrollo de la nación como factores multiplicadores de los efectos de las señaladas amenazas, sean estas tradicionales o emergentes, incluyéndose todos aquellos riesgos provenientes del ciberespacio, habiéndose presentado diversos informes para incentivar la protección del ciberespacio, así como el Reporte de seguridad cibernética y la infraestructura crítica de las Américas (2015) y las Tendencias en la ciberseguridad de las Américas y el Caribe, respuestas de los países (2013).

Los riesgos están definidos en el vocabulario militar como la contingencia o la proximidad de un daño, como también de cualquier otro factor o situación que pueda impedir la ejecución de un plan propio o que permita al adversario ejecutar su plan. Además, incluye en el riesgo de una operación militar a cualquier condición real o potencial que involucre acciones inminentes del adversario que puedan causar daño o muerte a los individuos implicados en una operación. De la misma manera, durante el desarrollo de los enfrentamientos en el campo de batalla estos riesgos normalmente se presentarán de diferente forma o causando disímiles niveles de afectación, pudiendo ser estratégicos, operacionales o tácticos², generales o localizados en partes específicas del escenario, pudiendo constituirse alguno de ellos en una seria amenaza a la existencia o a la capacidad de operar con normalidad, existiendo vulnerabilidades y las interferencias que pueden catalizar el éxito que se requiere como efecto deseado en la confrontación militar.

Las experiencias recientes en el ámbito de las acciones conjuntas frente a amenazas ocurridas en el ámbito de la ciberguerra y del ciberespacio recomiendan a los comandantes evaluar de forma permanente los riesgos existentes, con el objeto de adoptar las medidas necesarias para mitigar y prevenir anticipadamente sus efectos.

Existe un consenso general de que estas situaciones de vulnerabilidad se originan en el adversario, los aliados y desde dentro de la propia organización militar, por lo que este manejo del riesgo estará presente en los distintos modelos de la apreciación de la situación, para poder identificar los peligros y minimizar sus efectos en forma de riesgos controlados y ser aceptados por la decisión del propio comandante, procedimiento que colaborará a la eficiencia operacional de la unidad y que aportará una mayor probabilidad de éxito en el cumplimiento de la misión³.

Según el Ejército de EE.UU., los riesgos en el ciberespacio pueden ser técnicos, operacionales o de la política normativa. De ellos nace la necesidad de hacer frente a los riesgos y amenazas con operaciones ofensivas y defensivas

² US Army War College, Strategic Studies Institute (SSI), NATO cyberspace capability: an strategic and operational evolution, EE.UU., 2016, pp. 10-11.

³ *Ibíd.*, pp. 3-14.

en el ciberespacio, las que dependerán del entrenamiento de las unidades y del personal y de las capacidades necesarias para mitigar los efectos de la acción adversaria.

Debido a que los ciberriesgos y las ciberamenazas presentes en el dominio ciberespacial son cada día más frecuentes y avanzadas, adoptar medidas de seguridad activas y pasivas para prevenir y enfrentar directamente sus acciones se constituye en una obligación en cualquier estructura militar factible de recibir acciones ofensivas de ciberguerra, por lo que gestionar un plan de contingencia que enfrenten estas crisis cibernéticas y evitar fugas masivas de información o que afecten los sistemas de mando y de control de las operaciones militares será indispensable de asumir y de prever, por cualquier organismo del sector defensa, por medio de las denominadas acciones de ciberdefensa y de ciberataque.

En la doctrina conjunta de Gran Bretaña y respecto de las “ciberamenazas”, se menciona el origen de las amenazas del ciberespacio, sus propiedades, formas y técnicas de los ciberataques que las concretan, señalando los diferentes niveles y actores que la configuran, y que poseen las siguientes características: vectores, códigos computacionales, comportamiento y efectos. Finaliza esta conceptualización de las amenazas con el ejemplo de ocho estudios de casos: personal que hurta información, manipulación del comercio en la *web*, ciberataques conducidos por ataques de grupos patrióticos, operaciones de ciberataque en períodos de tensión entre dos países, amenazas internas de la organización, el impacto de la encriptación, el impacto de virus en las capacidades militares e ingeniería social con propósitos de espionaje⁴, lo que refleja el grado de detalle que este país ha alcanzado en su reglamentación conjunta de forma totalmente integrada a la comunidad nacional del ciberespacio.

Conforme con lo anterior, el concepto de riesgos o interferencias en el ámbito de la defensa debería reservarse para aludir de manera precisa a los fenómenos cuyas características reflejan mejor los rasgos de lo que constituye una amenaza propiamente tal, entre otras, la existencia de un actor internacional que manifiesta su voluntad de causar daño a los intereses nacionales y que tiene la capacidad de materializarlo. A diferencia de esta visión de la defensa, las amenazas emergentes caen en una categoría más amplia, de problemas de seguridad, en que se incluyen fenómenos como el terrorismo, narcotráfico, proliferación de armas de destrucción masiva, pobreza, pandemias, ataques cibernéticos y otros, que no constituyen parte de amenazas convencionales

⁴ Development, Concepts and Doctrine Centre (DCDC), *Cyber Primer, Second Edition*, Ministry of Defense, UK, 2016, pp. 19-33.

propriadamente tal, aunque eventualmente pueden transformarse y evolucionar por la globalidad de sus efectos en la comunidad nacional.

Las ciberamenazas a los sectores ajenos a la defensa, cuyas respuestas preventivas e investigativas corresponden al ámbito de la seguridad pública, han afectado a grandes compañías nacionales o extranjeras, frecuentemente causando daños medianos en los mercados e influyendo menormente en los rendimientos generales de las economías, sin haberse constituido todavía en un riesgo mayor a la existencia como tal o como una amenaza real a la supervivencia de una sociedad nacional. Sin embargo, la difusión, conocimiento y el estudio de estas acciones ofensivas y sus respuestas gubernamentales o privadas son un escenario adecuado para buscar experiencias y prevenir que hechos similares afecten los sistemas de mando y control nacionales y militares, que se constituyan en amenazas reales a la fuerza en el nivel estratégico y operacional. Ya sea por su destrucción física o por la degradación que pudiera presentarse en las capacidades de mando y de control, especialmente en los sistemas de comunicaciones o en el uso libre de riesgos de los sistemas de informaciones por red, fijas o inalámbricas.

Lo anterior genera la necesidad de desarrollar una capacidad militar de prevención, detección y de respuesta ante las ciberamenazas, la que debe tener como objetivo fundamental el incrementar las fortalezas de análisis, explotación, respuesta, defensa, recuperación y coordinación antes estas acciones adversarias, haciendo énfasis en la protección de la administración pública, las infraestructuras críticas, las capacidades militares y de defensa, como de otros sistemas nacionales de interés nacional⁵. Esto genera agentes, estados, acciones de ataque y de defensa en la lucha por el control de la información en el ciberespacio mundial, generando riesgos y amenazas en quienes manejan y administran los recursos financieros e informáticos, agrupándose en diferentes sectores o áreas del quehacer nacional, que da origen a la infraestructura crítica de la ciberseguridad, y que para los fines de este trabajo puede ser separada por los siguientes niveles, nacional, sectorial o de la defensa en lo ministerial, conjunto, institucional y operacional, con el propósito de determinar los efectos de la guerra por el mando y control en la ciberguerra.

Un importante aspecto a tener en consideración para tiempo de paz, crisis o de guerra, es que gran parte de las amenazas, riesgos y vulnerabilidades de la infraestructura crítica del sector de la defensa, o de los niveles de la conducción militar estratégico y operacional, proviene de la existencia

⁵ Instituto de Estudios Estratégicos de España (IEEES), Cuaderno de Estrategia N° 185, Ciberseguridad, la cooperación público-privada, España, 2016, p. 148.

en forma permanente de amenazas o por la generación de riesgos inesperados en aquellos sectores del ámbito privado, cuyos recursos o beneficios de instalación son utilizados por el sector público o por las instituciones militares, ya que gran parte de las estructuras de la defensa son usuarias de tecnologías de información y de comunicaciones de uso civil, los que padecen de defectos de diseño en materia de seguridad, debido principalmente a los tiempos del mercado y la presión de los inversores⁶. Muchos de los sistemas logísticos y administrativos dependen de la existencia de servicios básicos de índole privado, de la provisión de alimentos provenientes de proveedores nacionales o internacionales, contratistas de seguridad, servicios externos de transporte internacionalizados e incluso las oficinas de finanzas, el personal y sus familias dependen totalmente del funcionamiento de complejas redes financieras que funcionan totalmente en la *web* privada o en sistemas informáticos complejos, clasificándose los riesgos en operacionales, técnicos y riesgos en el cumplimiento de las políticas⁷.

La infraestructura crítica en la ciberguerra

La infraestructura crítica es una colección de sistemas y activos tanto tangibles como intangibles que proporcionan servicios críticos a la nación y su protección debe ser dirigida para asegurar la confiabilidad y la continuidad a los servicios vitales en la salud, el transporte, de energía y otros ámbitos⁸. Estos sectores cubren todas aquellas áreas del acontecer nacional que se comportan como vitales, y que por su funcionamiento y buen servicio hacia la comunidad son requisitos para la supervivencia de la nación, como la banca, el comercio, los servicios básicos, el transporte aéreo, terrestre y marítimo, y muchos otros que aportan al bien común de los ciudadanos, debiendo considerarse a la Defensa Nacional como uno de los factores importantes de todo país, ya que su estructura superior como sector y por la existencia de las capacidades de las instituciones armadas, genera hacia los otros sectores las condiciones necesarias de seguridad y de normalidad que propician en forma equilibrada, evidente, colaborativa y recíproca el desarrollo nacional.

Según la Unión Europea (UE), la conceptualización de infraestructura crítica señala que “incluye aquellos recursos físicos, servicios, infraestructuras de tecnologías de la información, redes y activos cuya destrucción o

⁶ US Army, FM 3-12, Cyberspace and Electronic Warfare Operations, 2017, pp. 1-19.

⁷ *Ibid.*, pp. 1-20.

⁸ US Army War College, Strategic Studies Institute (SSI), Volumen III, Cyber Infrastructure Protection, 2017, pp. 199-200.

interrupción podría tener un serio impacto en la salud, seguridad o bienestar económico de los ciudadanos, o en el funcionamiento eficaz de los gobiernos. Hay tres grupos de activos de las infraestructuras, de los que uno de ellos está compuesto por los activos públicos y privados y sus redes físicas y lógicas (ciberredes o ciberespacio) interdependientes”⁹. En esta misma publicación se agrega el concepto de servicio esencial, el que sin un sector crítico puede presentar diversas vulnerabilidades que afecten el funcionamiento normal de la sociedad afectando la seguridad de las personas y la seguridad total de la nación. Son “aquellos servicios básicos como el agua, gas, electricidad, etc., junto con otros como los sistemas eléctricos, sistemas de control medioambiental o redes de comunicaciones que interrumpidas ponen en riesgo la seguridad y confianza pública, amenazan la seguridad económica o impiden la continuidad del gobierno de los Estados miembro o sus servicios”. Finalmente, se define en este ámbito a la infraestructura de información crítica como los “sistemas tecnológicos, de información y de comunicaciones que son infraestructuras críticas en sí, o que son esenciales para la operación de otras infraestructuras críticas (telecomunicaciones, ordenadores/*software*, Internet, satélites, etc.)”¹⁰, lo que refleja una buena conceptualización de los diversos componentes nacionales que pueden ser afectados por los distintos riesgos o amenazas.

La Política Nacional de Infraestructura Crítica de EE.UU.¹¹ señala que proporciona a la nación los servicios esenciales que sustentan a la sociedad americana, para ello se requieren esfuerzos proactivos y coordinados para fortalecer y mantener una infraestructura crítica segura, funcional y resistente, que incluye todos los sistemas vitales para la confianza de la comunidad nacional y para la seguridad, prosperidad y el bien común de la sociedad americana. Esta es diversa y compleja, considerando redes y sus canales de distribución, estructuras organizativas variadas y modelos operativos, funciones y sistemas interdependientes, tanto en el espacio físico como en el ciberespacio y estructuras de gobierno que involucran autoridades, responsabilidades y regulaciones en todos los niveles.

Por otra parte, el Plan de Protección de Infraestructura Crítica de Canadá¹², con las políticas de desarrollo hasta el 2017, incluye como áreas del sector público y privado a ser fortalecidas y protegidas desde el nivel central

⁹ Oscar Pastor Acosta y otros, Seguridad Nacional y Ciberdefensa, Fundación Rogelio para el desarrollo de las telecomunicaciones, Madrid, 2009, p. 110.

¹⁰ *Ibíd.*

¹¹ Presidential Policy Directive PPD-21, Critical Infrastructure Security and Resilience, EE.UU., 2013, pp. 1-2.

¹² Government of Canada, Action Plan for Critical Infrastructure, Canada, 2014, p. 11.

gubernamental a las siguientes: energía y servicios básicos, información, comunicación y tecnología, finanzas, salud, alimentación, agua, transportes, seguridad, gobierno y manufactura.

Ten y Liu, en *Cybersecurity for critical infrastructures: attack and defense modeling*, definen la infraestructura crítica de la ciberseguridad como “los sistemas físicos y sistemas computacionales complejos que forman parte importante de una sociedad moderna y su funcionamiento fiable y seguro, es de suma importancia para la vida económica y la seguridad nacional”¹³. Esta última definición corresponde al ámbito civil preferentemente y se relaciona a nivel estatal con la ausencia de amenazas y riesgos para el normal funcionamiento de los sectores denominados críticos que establecen las políticas nacionales, indicando normalmente a “la energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otros, debido a que los países deben actualizar en forma permanente los mapas de riesgos y las amenazas del ciberespacio, porque cualquier error o ataque exitoso vulnerará el bienestar y los derechos de la comunidad, perjudicando los intereses particulares y comunes, afectando con ello el funcionamiento de los servicios críticos de la nación, lo que vincula esta infraestructura con el nivel nacional por sus posibles amenazas y efectos.

Por otra parte, también se ha establecido “que numerosos estudios e investigaciones han caracterizado al ciberespacio como un dominio de naturaleza militar, y en esta línea, la conveniencia de desarrollar capacidades militares de ciberdefensa por parte de los Estados ha pasado a ocupar cada vez más espacios en los debates prospectivos acerca de la Defensa Nacional y el diseño de las fuerzas militares. En donde a diferencia de los tradicionales escenarios de batallas, tierra, mar, aire y el espacio, este nuevo dominio militar, no es físico, sino virtual”¹⁴. Con esta mención, se abre una variedad de posibilidades, ya que las amenazas del ciberespacio a los ámbitos militares de las operaciones durante tiempo de guerra serán respondidas física o virtualmente en los diferentes escenarios existentes, incluso el virtual, sea de manera defensiva u ofensiva. Ahora bien, qué pasaría si la infraestructura crítica o redes de la defensa nacional o militares son amenazadas en tiempos de paz por parte de autores desconocidos, sea proveniente de acciones desde

¹³ Juan Anabalón y Eric Donders, Revisión de ciberdefensa de infraestructura crítica, Estudios Seguridad y Defensa N° 3, ANEPE, 2014, p. 132.

¹⁴ Sergio Eissa, Sol Gastaldi, Iván Poczynok y María Di Tullio, El Ciberespacio y sus implicancias en la Defensa Nacional, aproximaciones al caso argentino, VI Congreso de Relaciones Internacionales, La Plata, 2012, p. 1.

un grupo internacional, un Estado contendor o de individuos ubicados en cualquier parte del planeta.

Normalmente las conceptualizaciones de infraestructura crítica señalan a la defensa como uno de los sectores de la ciberseguridad que pudieran afectar a la seguridad nacional, junto con otras áreas del quehacer público o privado y que son permanentes, ya que están dirigidas al bien común general de la población y a su bienestar. En este sentido, todo lo que puede afectar en tiempo de paz o de guerra a la operabilidad de las fuerzas militares, como asimismo a la preparación y ejecución de las operaciones en situación de conflicto armado, afectarán principalmente los sistemas de mando y de control de las unidades que dirigen las tropas, pero es posible señalar que también muchos otros sectores señalados y que pertenecen al ámbito externo pueden afectar las operaciones militares en el nivel estratégico y operacional, aunque sean de origen civil, en ello se destacan los sectores del transporte, energía, salud y seguridad pública, que pueden darse en las zonas de retaguardia o en la zona del interior de un teatro de guerra, provocando efectos negativos en las zonas de operaciones y los frentes de combate.

Se considera que los ataques cibernéticos que afectan a la Defensa Nacional estarán orientados principalmente hacia algunos de los siguientes objetivos: quebrantar la infraestructura del enemigo, la logística y las cadenas de suministro. Distraer, confundir e inhabilitar el sistema de comando, control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento. Negar capacidades similares del adversario y crear oportunidades para ataques estratégicos en la infraestructura del enemigo¹⁵. Un aspecto especial está señalado por los efectos que puede tener un ataque cibernético a la industria de la defensa nacional, además de otros proveedores de materiales sensibles al interior del territorio que pudieran constituirse en equipos o elementos necesarios o indispensables para sostener un probable esfuerzo de guerra, como combustibles, municiones, repuestos, productos de primera necesidad para la alimentación, cuya falta o mal funcionamiento pudieran tener efectos en el desarrollo o el éxito de las operaciones militares.

Buscando tener una referencia de cuáles son las amenazas o las agresiones relacionadas con la ciberseguridad que pueden afectar a la Defensa Nacional, se tuvo a la vista lo expresado por el Comandante del Mando Conjunto de Ciberdefensa (MCCD) de España. Él indica que estas relaciones son asimétricas, vale decir, un Estado o alguien muy grande puede sufrir ataques y daños de otro agente muy pequeño, lo que abre las posibilidades y el rango de las amenazas y agresiones al sector de la defensa a una cantidad enorme y

¹⁵ *Ibíd.*, p. 9.

probable de situaciones, con lo que un grupo terrorista, una mafia organizada o incluso un Estado por muy pequeño que sea, podría tener la capacidad de infringir un daño en un sistema de información de un país grande¹⁶. Esta aproximación resulta interesante respecto de cuáles son los ámbitos prioritarios de la acción del Mando Conjunto de Ciberdefensa, señalando que esta unidad nace el 2013 para proteger los sistemas de información y de comunicaciones del Ministerio de Defensa y de las Fuerzas Armadas, lo que ubica su acción en el ámbito político de la Defensa Nacional y estratégico/operacional de las acciones militares, poniendo énfasis en las operaciones que España realiza en el exterior del país, en situaciones distintas a la guerra y de apoyo a la política exterior del país, OTAN o la Unión Europea. En otros aspectos de su entrevista, delimita cuáles serán las respuestas militares ante un ataque cibernético hacia entidades civiles o de su propio ámbito, “si se produce un ciberataque en un sistema militar, sería de responsabilidad del Mando Conjunto de Ciberdefensa”, tomar las acciones defensivas y ofensivas que la situación y la propia seguridad del país amerite.

Efectos de la ciberguerra en la infraestructura crítica

Conceptualmente los efectos se relacionan con las repercusiones que determinadas acciones positivas o pasivas pueden tener en la normalidad de una estructura, un sistema, empresa o instituciones, las que desde un punto de vista militar se pueden relacionar con los diferentes niveles de la conducción militar: estratégico, operacional y táctico, en cuanto a la validez e influencia de sus resultados en la continuidad y futuro de las operaciones, ya que el efecto deseado es el estado final buscado por toda acción militar, terrestre, naval o aérea. En este sentido el diccionario militar reconoce los efectos de amarrar, aislar, degradar, detener, encauzar, engañar, fijar, interditar, retardar, destruir, hostigar, de los fuegos y neutralizar dentro de las tareas tácticas propias de una planificación de detalle. Estas repercusiones pueden ser físicas, involucrar la pérdida de vidas humanas o ser conceptuales, ocasionando graves daños en la población civil o incluso atentar gravemente al bienestar o el bien común general de la comunidad, sin mencionar los efectos en los sectores críticos descritos en la infraestructura nacional, donde la Defensa Nacional como parte de la infraestructura estará incluida junto con otras áreas sensibles del país.

¹⁶ Carlos Medina, Critical infrastructure, cybersecurity, industry and defense, GM News N° 56, España, 2014, pp. 9-10.

Además, se debe tener en cuenta que muchos otros eventos de menor afectación o técnicos, sean ellos tangibles, propios y característicos de las operaciones militares o intangibles, que afecten los sistemas de mando y control del nivel táctico en el ciberespacio, pueden desencadenar efectos de carácter estratégicos e incluso políticos, escalando sus repercusiones hasta los mayores niveles del país, según sea la importancia que tiene para el devenir de la nación o la población del país, pudiendo darse en tiempos de normalidad, de crisis o de conflicto armado frente a otro Estado, ya que los ciberataques o el ambiente de ciberguerra puede presentarse durante la paz, y de igual forma afectar seriamente a la seguridad global por sus efectos, en donde obviamente la Defensa Nacional deberá responder o al menos prestar asesoría a las máximas autoridades gubernamentales en la búsqueda de soluciones desde su propio ámbito de acción, como ocurre en las principales doctrinas examinadas para este trabajo.

Los efectos en el ámbito del mando y control de las operaciones militares durante tiempos de crisis o de guerra se pueden presentar producto de acciones ofensivas o disruptivas en toda la amplitud del ciberespacio nacional, y cuyos resultados vulneren la normalidad de los diversos sectores identificados como parte de la infraestructura crítica en las respectivas políticas nacionales, por tener repercusiones importantes en la seguridad nacional, como también a la Defensa Nacional como sector, por los efectos que tienen las operaciones de ciberguerra de afectar la capacidad efectiva de comando y conducción de las tropas en los niveles estratégicos, operacionales y tácticos de las operaciones militares, situación doctrinaria de carácter política o militar que difiere en cada país o alianza regional.

Dentro de las acciones destinadas a la protección de las propias fuerzas y los contingentes aliados, existen aquellas que buscan disminuir las vulnerabilidades de los elementos físicos, electrónicos y de información por medio de operaciones y medidas de seguridad. Siendo que la infraestructura de información es difícil circunscribirla en términos físicos o con fronteras geográficas específicas, la prioridad de la protección de la información debe dirigirse a aquella en donde el adversario tiene la capacidad de afectarla, toda vez que simultáneamente es utilizada en la ejecución del propio mando y control.

El Foro Económico Mundial (World Economic Forum, por su sigla en inglés WEF) señala que las amenazas provenientes de los ciberataques es uno de los cinco riesgos más importantes que confronta a las naciones actualmente. De esta forma los ciberataques se incrementan en sus acciones hacia blancos ubicados en el núcleo central de las naciones y las diferentes

organizaciones gubernamentales y civiles que sufren estas nuevas fuentes de conflicto en el mundo globalizado actual, por ello, las amenazas de ataques a la infraestructura crítica, las interrupciones parciales o totales de los servicios básicos que la componen a nivel nacional, genera un amplio rango, un extremo y un creciente margen de dificultad para defenderse ante estas situaciones y generar las capacidades adecuadas por la amplitud de los riesgos existentes¹⁷.

La integración de todas las operaciones del ciberespacio y sus efectos en la búsqueda de objetivos nacionales, debe considerar la coordinación de todas las iniciativas y acciones de ciberataque y de ciberdefensa del Estado. En el ámbito de las operaciones militares, debe tener claridad acerca de los efectos estratégicos, operacionales, tácticos y los tiempos de ejecución. El comando y control de la ciberguerra es muy complejo de coordinar y de conducir, siendo la mezcla de diversos organismos nacionales y militares, según los objetivos entregados por la autoridad política y comportarse de acuerdo con los marcos entregados por la normativa y las estrategias nacionales. En Gran Bretaña este comando y control nacional se ejecuta por medio de ocho organismos civiles y siete organismos militares, lo que refleja la complejidad de las coordinaciones de las operaciones en este ámbito. Se señala al mando y control como parte integrante de la doctrina de ciberguerra en este país y se ejemplariza mediante diversos estudios de caso: operaciones ofensivas versus otro Estado en Irán, acciones de ciberataque en apoyo a operaciones convencionales por Israel y ciberataques por medio de afectaciones a la infraestructura nacional en Ucrania¹⁸, relacionando directamente al ciberespacio con la acción militar internacional respecto de componentes de la infraestructura crítica de un Estado contendor.

Dentro de las conceptualizaciones de los diferentes elementos del ciberespacio que han incorporado los distintos países y organismos internacionales, merecen una destacada importancia las que la OTAN ha implementado en su doctrina desde el 2002, en donde se mencionan las tres dimensiones, los cinco mandatos y los cinco dilemas de la ciberdefensa, elementos que ilustran en forma muy adecuada las complejidades de este nuevo dominio operacional, en que la defensa y la seguridad se puede ver afectada en su infraestructura crítica, tanto las pertenecientes a organizaciones de carácter privadas como las relacionadas con los organismos estatales. Las tres dimensiones

¹⁷ Thomas Johnson, *Cybersecurity protecting critical infrastructures from cyber attack and cyberwarfare*, CRC Press, EE.UU., 2015, ix.

¹⁸ Development, Concepts and Doctrine Centre (DCDC), *Cyber Primer, Second Edition*, Ministry of Defense, UK, 2016, 74-79.

son la gubernamental, la nacional y la internacional¹⁹. Los mandatos son lo cibermilitar, el contracibercrimen, la inteligencia y la contrainteligencia, la protección de la infraestructura crítica y el manejo de crisis nacional y la ciberdiplomacia y la gobernanza del internet. En cuanto a los cinco dilemas que presenta la ciberdefensa, se estructuran en estimular la economía versus mejorar la seguridad nacional, la modernización de infraestructura versus la protección de esta infraestructura crítica, el sector público versus el sector privado, la protección de datos versus compartir la información y finalmente la libertad de expresión versus la estabilidad política²⁰.

El análisis de lo establecido por la OTAN demuestra la complejidad de asumir estas tareas al más alto nivel de la estructura de la nación, en donde el sector defensa asume importantes responsabilidades de manera conjunta y combinada con socios estratégicos, como asimismo que la evidencia que muchos de estos desafíos y nuevas amenazas no son asumidos como una respuesta similar por todos los países de la misma manera, a pesar de las evidencia que demuestran los hechos, de que la ciberguerra es una de las más potentes amenazas del futuro y que afectan el bien común de las sociedades en tiempos de guerra y con ausencia de declaraciones de beligerancia o de operaciones tradicionales en el campo de batalla. He aquí la necesidad de asumir estos desafíos generando políticas y estrategias, organizando medios, asignando recursos, elaborando doctrinas, preparando personal y adquiriendo medios materiales para enfrentar adecuadamente este flagelo del futuro que no tiene siempre una cara visible.

El uso de las capacidades de ciberguerra de un actor o un grupo internacional se verá traducido en acciones de un ciberataque hacia diversos sistemas de la infraestructura crítica, en ocasiones hacia los sistemas de mando y control gubernamentales o estratégico-militares, siendo este término usado indistintamente por varios países, ya que no hay una uniformidad conceptual para definirlo, existiendo muchas diferencias incluso dentro de una sola nación, siendo la más general el referirse a un ataque cibernético, como el intento malicioso y premeditado de interrumpir la confidencialidad, integridad o disponibilidad de información que residen en computadoras o servidores de redes, en donde se verifica la importancia de la libertad de acción para usar la propia información sin restricciones, atenuando o eliminando la existencia de riesgos reales o potenciales, asimismo, ello es tan importante como denegarla al uso del adversario evitando cualquier intención de ataque, reflexión que

¹⁹ NATO, National Cybersecurity Framework Manual, Cyber terms and definition, CCDCOE, Estonia, 2012, p. 29.

²⁰ *Ibid.*, pp. 34-41.

por supuesto incluye el uso libre de interferencias de los sistemas de mando y control en las operaciones militares.

Se ha evidenciado que el ciberespacio es un nuevo campo de batalla donde ocurrirán acciones que ponen en riesgo a las comunidades nacionales amenazando su seguridad y la continuidad de sus políticas en procura del bien común de la sociedad, con la aparición de ataques a organismos civiles, estatales o militares de la estructura nacional, lo que tendrá cada vez más relevancia, como ha quedado señalado por las tendencias estratégicas internacionales del ciberespacio, para ello se debe hacer frente a los desafíos y dilemas que este nuevo tipo de guerra presenta a las autoridades y a los medios de la defensa nacional. Lo anterior, ya que estos ciberataques son el resultado de un nuevo tipo de arma silenciosa, barata, anónima y que proviene de una red en cualquier parte del mundo y que puede tener efectos gigantescos en las economías, sectores financieros, productivos, de manufacturas o proveedores de los servicios básicos de sus habitantes.

Otro de los efectos de los riesgos y amenazas en la ciberguerra, impone que la respuesta nacional debe ser proactiva y anticipatoria, cubriendo desde lo político toda la estructura gubernamental hasta el nivel operacional del campo de batalla, ya que por cualquier flanco o espalda del dispositivo puede aparecer un riesgo o una amenaza, la que se propagará hacia los medios superiores o vecinos afectando el mando y el control de las operaciones militares, o incluso la transmisión de órdenes y la supervisión de la planificación que se haya impartido, siendo muy probable que afecte la operacionalidad de una fuerza sin sufrir siquiera una baja en combate por la acción de las armas de fuego o de algún artificio mecánico.

Las acciones que el Estado acometa sin duda tendrán un efecto en la sociedad, ya que la libertad y los derechos básicos de las personas se verán afectados como lo señala uno de los dilemas de la OTAN. Existe una contradicción entre proteger la información y compartirla, pero esta situación rápidamente tiene una respuesta fácil de asumir por la autoridad o los mandos militares, si es que está en riesgo, por ejemplo, el funcionamiento del sistema financiero, el transporte o las comunicaciones del país, cuyo mal servicio por horas, días, semanas o meses tendrán un efecto catastrófico más importante que una bomba en plena bolsa de valores o de comercio de cualquier país en el mundo. Al mismo nivel que la mención anterior se encuentra la protección de los servicios básicos de energía, luz, combustibles y de alimentación, ya que sus efectos negativos de afectación son prácticamente inmediatos, y que por cierto influirán en cualquier operación militar en el campo de batalla tradicional, donde se desenvuelven los tanques, los aviones o los buques de guerra actualmente.

Una de las particularidades de los efectos que tiene la ciberguerra son los denominados problemas de atribución²¹, ya que un “ciberataque no siempre dejará rastros de su origen”, en este sentido se asevera “que los países atacados se ven en la necesidad de gestionar las consecuencias del ataque, pero también de articular de manera inmediata una respuesta frente a una agresión que procede de diferentes puntos del planeta, sin que pueda conocerse la culpabilidad real de cada uno de los equipos atacantes”, esta complejidad presenta una dificultad jurídica y forense, toda vez que para tomar medidas efectivas deberá conocerse el origen y la causa de la amenaza o la afectación sufrida, la que muchas veces es difícil de determinar de una manera científica con la rapidez que imponen los acontecimientos, estableciéndose la necesidad de generar métodos especializados de carácter preventivos o reactivos.

En la guerra convencional, la disuasión ocupa un importante lugar, ya que la posesión de capacidades militares de carácter defensivas y ofensivas imponen un aporte estratégico que deberá tenerse en consideración cuando se pretenda disputar un objetivo político, económico, geográfico o militar. Considerando lo anterior, un efecto importante que se genera producto de las acciones de ciberguerra contra la infraestructura crítica de carácter nacional es que la disuasión pierde una de sus condiciones más válidas, que es la credibilidad y la oportunidad de su respuesta para recuperar la libertad de acción, ya que si se desconoce el origen de la amenaza o si el ciberataque tiene su origen en un individuo o un grupo localizado en el otro lado del planeta, un Estado posee pocas herramientas para hacer sentir sus instrumentos del poder nacional como una respuesta apropiada, siendo un aspecto que está estudiándose a nivel global, especialmente para hacer frente a aquellos ataques provenientes de grupos terroristas internacionales desde lugares remotos. En este sentido, se ha señalado que “la disuasión es compleja y no se limita solo a represalias, ya que en el ámbito de la ciberguerra existe la posibilidad de generar una disuasión que vaya más allá del desarrollo de capacidades ofensivas de respuesta inmediata, por ejemplo desarrollar alternativas que consisten en proteger los ciberintereses mediante defensas activas que permitan que el atacante se infrinja a sí mismo el daño que desea causar”²².

Las acciones propias de la ciberguerra tienen efectos en la infraestructura crítica de una nación, lo que perjudica las capacidades de dirección de la estructura nacional o de conducción de la fuerza militar. Esta situación claramente repercute en la seguridad de un país, siendo necesario, en este particular contexto, el involucramiento del sector defensa y de las instituciones

²¹ Javier Jordan, *Manual de Estudios Estratégicos y Seguridad Internacional*, Capítulo de la Ciberguerra de Manuel Torres, Plaza y Valdés Editores, España, 2013, pp. 334-335.

²² *Ibid.*, pp. 345-346.

militares para la preparación y ejecución de medidas defensivas y ofensivas, que permitan obtener una capacidad de ciberdefensa adecuada, que atenúe los riesgos y amenazas existentes. Se considera que los ataques cibernéticos que afectan a la defensa nacional “están orientados por los siguientes objetivos: quebrantar la infraestructura logística y cadenas de suministro. Distracer, confundir e inhabilitar el sistema de comando, control, comunicaciones, computación, inteligencia, vigilancia y reconocimiento. Negar las capacidades similares del enemigo y crear oportunidades para ataques estratégicos en las infraestructuras del enemigo”²³. Obviamente, ante este planteamiento, al igual que muchos países que poseen legislaciones internas que le permiten a las Fuerzas Armadas operar en acciones de seguridad interior durante tiempos de paz o ante catástrofes y emergencias, deberá existir a futuro una normativa legal que considere la acción militar en acciones distintas a la guerra, ante ciberataques como los señalados.

A nivel operacional y táctico en las operaciones militares, se harán sentir los efectos generados y producidos a nivel político en todo o parte del territorio nacional, como aquellos ocurridos desde el nivel estratégico conjunto en la conducción militar de la guerra, o en operaciones de tiempo de paz ante emergencias y catástrofes, e incluso en operaciones internacionales. Así, en situaciones de normalidad nacional las repercusiones, daños o mal funcionamiento de la infraestructura crítica nacional del sector eléctrico, combustible y transporte, entre otros, afectarán las comunicaciones y la conducción de los esfuerzos nacionales para sacar adelante el país.

En las operaciones militares distintas a la guerra, para desarrollar diferentes acciones humanitarias ante casos inesperados de emergencias o catástrofes nacionales, indistintamente del país donde se efectuó este apoyo a la normalización de la situación interna del territorio afectado, la función de mando y control adquiere relevancia, ya que se deben establecer enlaces permanentes entre los medios militares, las agencias del Estado, las autoridades nacionales, regionales, provinciales y comunales, las organizaciones no gubernamentales y la población civil, en esta situación de extrema vulnerabilidad se debe evitar la aparición de amenazas o de riesgos en la infraestructura crítica producto de la acción de individuos, grupos o Estados extranjeros, los que podrían tratar de imponer sus capacidades de ciberguerra en situaciones de debilidad. La recuperación de la normalidad en los sistemas de mando y control es la primera prioridad ante situaciones de emergencia, con el objeto de permitir posteriormente la recuperación del ambiente operacional y social que vivía

²³ Sergio Eissa, Sol Gastaldi, Iván Poczynok y María Di Tullio, *El Ciberespacio y sus implicancias en la Defensa Nacional, aproximaciones al caso argentino*, VI Congreso de Relaciones Internacionales, La Plata, 2012, p. 9.

el territorio afectado, ello mediante la acción de la fuerza militar en apoyo al bien común nacional y las autoridades, según los distintas normativas nacionales que dispongan estas funciones.

Queda en evidencia que la protección de la infraestructura crítica orienta a contar con políticas que incluyen al sector defensa como parte integrante de la colaboración público y privada, la que se ha estructurado para asumir en forma centralizada la planificación de las acciones e iniciativas que coloquen al país en condiciones aceptables para enfrentar los desafíos que significa reducir los riesgos y enfrentar las distintas amenazas a la seguridad nacional o el bien común de sus ciudadanos que pueden provenir desde el ciberespacio. Estos desafíos han sido catalogados en forma detallada por estos planes y políticas, siendo un ejemplo de ello la evidencia de la existencia de tendencias de futuro y prospectivas en el ambiente internacional de la ciberdefensa y la ciberguerra, con el propósito de desarrollar adecuada y preventivamente diversas áreas a nivel nacional y en la fuerza militar, con el objeto de mantener capacidades en las distintas estructuras gubernamentales y de la defensa nacional²⁴.

Estas capacidades nacionales para enfrentar la protección de la infraestructura crítica antes las amenazas de la ciberguerra son las siguientes: poseer material suficiente y moderno para asumir los cambios tecnológicos y las tareas de cada sector nacional, infraestructura para que las instalaciones y material cuenten con la debida protección y seguridad física, recurso humano civil y militar capacitado en suficiente fuerza y permanencia de continuidad para enfrentar los desafíos y tareas, educación y capacitación permanente en materias de ciberdefensa y en tecnologías de información participando activamente en entrenamientos y ejercicios nacionales e internacionales, doctrina nacional y conjunta que permita una sinergia de las capacidades de los distintos entes nacionales públicos y privados, como de las instituciones de la Defensa Nacional, organización adecuada en los distintos niveles políticos, ministeriales, estratégicos y operacionales conjuntos, institucionales o en las áreas jurisdiccionales de las zonas de operaciones terrestres, navales o aéreas, para finalmente articular una eficiente colaboración público y privada que fortalezca la resistencia ante los riesgos y las amenazas internas o externas.

Un aspecto que debe ser destacado tiene su origen en el género humano, ya que existe un desconocimiento o una incredulidad de que los efectos de las amenazas de ciberguerra en la infraestructura nacional no alcanzarán a toda la ciudadanía o a toda la organización militar. Entonces, los ciudadanos o los

²⁴ Centro de Estudios Superiores de la Defensa Nacional (CESEDEN), Monografía N° 126, El ciberespacio, nuevo escenario de confrontación, capacidades para defensa en el ciberespacio, España, 2012, pp. 244-246.

integrantes de la defensa no evidencian adecuadamente en forma individual, por un aspecto de tipo psicológico, la real magnitud de los riesgos originados por este nuevo dominio operacional, por lo que no es asumido como una verdadera amenaza y, por esta razón, no es enfrentado como un desafío de futuro en forma proactiva y colectiva. Esto provoca que la capacitación y el adoctrinamiento de ciberguerra y de ciberdefensa en todos los niveles nacionales, políticos y militares sea una consecuencia del cambio de cultura que se debe producir por medio de una adecuada educación.

Habiéndose considerado la ciberguerra y sus efectos como una nueva amenaza del siglo XXI por diferentes organismos internacionales, ello ha generado efectos en las políticas nacionales y de defensa de los países desarrollados, ya que las acciones preventivas ciertamente involucran a la seguridad y la estructura de la defensa en el ámbito militar, ya que deben “afrentarlas decididamente, si no quieren convertirse en un objetivo fácil”, a pesar de la asimetría existente entre atacantes y defensores, existiendo una compleja y difusa línea entre ciberdelito, ciberterrorismo y ciberguerra²⁵. Las respuestas de la OTAN se han presentado desde la separación de las distintas redes de mando y control según su grado de confidencialidad, la creación de organismos especializados, el establecimiento de centros especializados y de doctrina, la cooperación internacional en ciberdefensa, la instrucción, formación, capacitación y entrenamiento en todo lo relacionado con la ciberguerra a nivel global y continental²⁶.

Lo anterior, por cierto, conlleva la existencia de un desafío nacional para afrontar el desarrollo de capacidades materiales y humanas, mediante la adquisición de equipos y la organización de unidades, procesos educativos que incorporen el estudio del ciberespacio, incorporación de nuevas tecnologías y doctrinas, el estudio y desarrollo de investigación aplicada y prospectiva, que aseguren una mejor seguridad para la nación, considerando la acción coordinada de todos los elementos del poder nacional, entre ellas, a las instituciones de la defensa, sin dejar de lado la implementación de planes que consideren acciones de ciberataque y ciberdefensa, para hacer frente a cada amenaza o contingencias que recomienden los estudios de riesgos, evitando interferencias y vulnerabilidades en los sistemas.

²⁵ Juan José Díaz del Río, *La ciberseguridad en el ámbito militar, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio*, Cuadernos de Estrategia N° 149, IUGM, Madrid, 2010, p. 219.

²⁶ NATO, National Cybersecurity Framework Manual, *Cyber terms and definition*, CCDCOE, Estonia, 2012, p. xiii.

Reflexiones finales

La comunidad internacional y las sociedades nacionales están expuestas en la actualidad a las vulnerabilidades de los sistemas en red y a las amenazas que se ciernen anónimamente sobre este quinto dominio intangible de la ciberguerra, afectando los diferentes sectores de la infraestructura nacional y los sistemas de comunicaciones en que se respaldan, ya que gran parte de sus servicios básicos y el funcionamiento del comercio, la industria y la banca, descansan en complejos equipamientos de *software* y de *hardware*, cables, enlaces satelitales o microondas, mediante los cuales también se producen los enlaces y se ejerce el mando, control y la transmisión de órdenes en el plano militar de las operaciones de guerra o distintas a la guerra, como también se procura el desarrollo nacional mediante el funcionamiento de todas las actividades económicas y sociales de una nación.

De esta forma, la presencia de riesgos y de amenazas de ciberguerra generan situaciones de vulnerabilidad que pueden afectar cualquiera de los componentes esenciales de la infraestructura crítica nacional, perjudicando el funcionamiento de los sistema de mando y control gubernamental y militar, eventos repentinos que pueden presentarse en períodos de normalidad constitucional, o en situación de emergencia, crisis o de guerra, anormalidad que impedirá la trasmisión de órdenes, el control y la dirección de los medios de la fuerza militar propia o mantener un panorama actualizado de la situación general que se vive en el territorio nacional o en el teatro de operaciones.

Además, sin que existan riesgos externos o internos evidentes que amenacen la seguridad nacional, pueden presentarse ataques informáticos de ciberguerra a los diferentes componentes civiles o militares del Estado, que pueden afectar a la población y la operacionalidad de las fuerzas militares, con ataques cibernéticos que pueden desencadenar una situación de extrema gravedad que haga necesario transitar a la utilización de medios militares de manera ofensiva o defensiva en el ciberespacio. En las ocasiones que los ataques o riesgos que se presenten en un ciberataque sean de bajo nivel, alcance o de repercusiones acotadas, la acción de las policías y los medios especializados cibernéticos del Estado serán suficientes y bastarán para hacer frente a esta situación de manera reactiva o con la imposición de la legalidad existente.

La infraestructura crítica y los medios del sector defensa que lo componen, al verse afectados repercuten directamente en la seguridad de una nación, situación y recursos que deben ser protegidos con medidas activas y pasivas mediante acciones de ciberataque o de ciberdefensa, las que muchas veces se efectuarán como represalia o de una manera preventiva con acciones ofensivas, siendo algunas de ellas factibles de tener que ser ejecutadas

afuera del territorio nacional, cuando la legislación de estas naciones así se lo permita a la fuerza militar o a los organismos del Estado encargados de estas funciones. Esta capacidad de ciberrespuesta en cualquier parte del mundo o la voluntad política de materializar una respuesta militar ante ataques externos, proporcionará una cobertura especial de carácter disuasiva que tiene validez ante adversarios o entes conocidos, pero será escasa ante individuos o grupos anónimos.

El sector defensa y las instituciones de la defensa constituyen una parte importante de la infraestructura crítica nacional, y como tal, este sector puede verse igualmente afectado por las amenazas internas o externas provenientes de ataques cibernéticos, los que indudablemente se concentrarán en los sistemas de mando y control, con el objeto de impedir la ejecución de los procesos de planificación y de conducción de los medios en las operaciones militares de guerra o distintas de la guerra. También, esta acción física o intangible por medio del ciberespacio sobre el mando y control de las operaciones militares repercutirá en los procesos logísticos y administrativos que se ejecutan en la zona de comunicaciones y la zona del interior, recibiendo además los efectos negativos que los servicios externalizados nacionales proveen, los que al verse perjudicados por las fallas en la infraestructura crítica nacional también influirán en el rendimiento institucional, así como combustible, energía, transporte, etcétera.

Los efectos de las acciones de ciberguerra en la infraestructura crítica perturbarán principalmente los sistemas de mando y control, ya que allí residen los riesgos, amenazas y objetivos del ciberataque adversario, por lo que esta situación de vulnerabilidad redundará en la operabilidad de los medios militares, sin diferenciar que estos ataques provengan de Estados, grupos o individuos, ya que puede tener efectos catastróficos en la sociedad si se ven afectados los servicios básicos, los sistemas de comunicaciones de la empresa privada y del gobierno o los sistemas militares del nivel ministerial o conjunto, teniendo como resultado una situación de incertidumbre y de desconcierto, que generará una gran convulsión social afectando el bien común y la normalidad de los procesos de desarrollo nacional.

Bibliografía

Anabalón, Juan y Donders, Eric. Revisión de ciberdefensa de infraestructura crítica, Estudios Seguridad y Defensa N° 3, ANEPE, Chile, 2014.

Centro de Estudios Superiores de la Defensa Nacional (CESEDEN). El ciberespacio, nuevo escenario de confrontación, capacidades para defensa en el ciberespacio, España, 2012.

- Development, Concepts and Doctrine Centre (DCDC), *Cyber Primer*, Second Edition, Ministry of Defensa, UK, 2016.
- Díaz del Río, Juan José. *La ciberseguridad en el ámbito militar*, Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio, Cuadernos de Estrategia N° 149, IUGM, Madrid, 2010.
- División Doctrina (DIVDOC), DD-10001, *Doctrina del Ejército y la Fuerza Terrestre*, Ejército de Chile, 2010.
- División Doctrina (DIVDOC), MDO-90906, *Manual Diccionario Militar*, Ejército de Chile, 2011.
- DoD initiates process to elevate US Cyber Command to Unified Combatant Command, declaración del Departamento de Defensa de los EE.UU. en www.defense.gov/news el 18AGO2017, EE.UU., 2017.
- Eissa, Sergio; Gastaldi, Sol; Poczynok, Iván y Di Tullio, María. *El Ciberespacio y sus implicancias en la Defensa Nacional, aproximaciones al caso argentino*, VI Congreso de Relaciones Internacionales, La Plata, 2012.
- European Parliament, *Global Trends to 2035, Geopolitics and International Power, Trend 7 Information Age and IV Cyber*, Bruselas, 2017.
- Government of Canada, *Action Plan for Critical Infrastructure*, Canada, 2014.
- Gray, Colin. *Making Strategic Sense of Cyber Power, why the sky is not falling*, US Army War College, Strategic Studies Institute, EE.UU., 2013.
- Instituto de Estudios Estratégicos de España (IEEES). *Cuaderno de Estrategia N° 185, Ciberseguridad, la cooperación público-privada*, España, 2016.
- Johnson, Thomas. *Cybersecurity protecting critical infrastructures from cyber attack and cyberwarfare*, CRC Press, EE.UU., 2015.
- Jordan, Javier. *Manual de Estudios Estratégicos y Seguridad Internacional, Capítulo de la Ciberguerra de Manuel Torres*, Plaza y Valdés Editores, España, 2013.
- Joint Chiefs Staff, Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, EE.UU., 1996.
- Laudicina, Paul. 2017 will be the year of cyber warfare, artículo disponible en www.forbes.com (Documento en línea) [Consultado el 16 de diciembre 2016].
- Medina, Carlos. *Critical infrastructure, cybersecurity, industry and defense*, GM News N° 56, España, 2014.
- NATO. *National Cybersecurity Framework Manual, Cyber terms and definition*, CCDCOE, Estonia, 2012.
- Organización de los Estados de América (OEA). *Declaración de Seguridad de las Américas*, 2003.
- Pastor Acosta, Oscar y otros. *Seguridad Nacional y Ciberdefensa*, Fundación Rogelio para el desarrollo de las telecomunicaciones, Madrid, 2009.
- Presidential Policy Directive PPD-21. *Critical Infrastructure Security and Resilience*, EE.UU., 2013.

La ciberguerra: sus impactos y desafíos

United Nations Security Council, Counter Terrorism Committee, Physical Protection of Critical Infrastructure against terrorist attack, CTED Trends Report, Nueva York, 2017.

US Army War College, Strategic Studies Institute (SSI), NATO Cyberspace Capability: an Strategic and Operational Evolution, EE.UU., 2016.

US Army War College, College Guide to National Security Issues, Volumen I, Theory of War and Strategy, Chapter 23 On the Theory of Cyberspace, EE.UU., 2012.

US Army, FM 3-12, Cyberspace and Electronic Warfare Operations, EE.UU., 2017.

US Army War College, Strategic Studies Institute (SSI), Volumen III. Cyber Infrastructure Protection, EE.UU., 2017.