LA CIBERGUERRA

SUS IMPACTOS Y DESAFÍOS

CEEAG
CENTRO DE ESTUDIOS ESTRATÉGICOS DE LA ACADÉMIA DE GUERRA
EJÉRCITO DE CHILE

LA CIBERGUERRA: SUS IMPACTOS Y DESAFÍOS

LA CIBERGUERRA: SUS IMPACTOS Y DESAFÍOS

Centro de Estudios Estratégicos CEEAG

Primera Edición, marzo 2018
100 ejemplares (tapa dura)
500 ejemplares (tapa rústica)
ISBN (tapa dura): 978-956-7734-09-2
ISBN (tapa rústica): 978-956-7734-08-5
Inscripción Registro de Propiedad Intelectual Nº A-290.357

Diseño de portada
Isabel Alcérreca Contardo

Diseño y diagramación
Andros Impresores

Impreso en Andros Impresores
Hecho en Chile / Printed in Chile

LA CIBERGUERRA:
SUS IMPACTOS Y DESAFÍOS

CEEAG
CENTRO DE ESTUDIOS ESTRATÉGICOS DE LA ACADEMIA DE GUERRA
EJÉRCITO DE CHILE

Índice

Dedicado a los alumnos y académicos de la Academia de Guerra.

Que las ideas expuestas en esta obra sirvan para ilustrar vuestro conocimiento y genere la necesaria curiosidad para un mejor discernimiento de la Defensa del presente y del futuro.

Prólogo

Durante el 2017 el Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile (CEEAG) desarrolló la investigación denominada "La Ciberguerra: sus impactos y desafíos". En este esfuerzo académico se asumió el desafío de conocer la complejidad de la ciberguerra porque contribuye a generar capacidades que incrementen el poder para accionar decisivamente en el campo de batalla, tanto en lo defensivo como en lo ofensivo, causando efectos operacionales y estratégicos que en numerosas oportunidades sobrepasan el ámbito militar y se proyectan a otros elementos del Estado como la población, la infraestructura vital e inclusive la moral nacional, solo por nombrar algunos.

El CEEAG, en cumplimiento al rol de generar conocimiento estratégico, anualmente publica un trabajo que es orientado por un tema de investigación central de la Academia de Guerra, tópico que es desarrollado por investigadores internos, siguiendo un lineamiento de análisis académico acorde con las áreas y subáreas de misión de la Defensa. Este texto se encuadra dentro de ello.

La ciberguerra se desarrolla fundamentalmente en el ciberespacio, sin embargo, algunas acciones contra la infraestructura destinada a su ejecución pueden llevarse a efecto en el ámbito terrestre, naval, aéreo y espacial. Es por eso que frente a un contexto tan amplio como el que configuran las dimensiones señaladas, esta investigación contribuye a generar conocimiento, en especial para Oficiales de Estado Mayor y Oficiales Ingenieros Politécnicos Militares del Ejército de Chile, para que así dispongan de una fuente de consulta para el estudio, análisis y la toma de decisiones respecto del empleo de la infraestructura de ciberguerra en las operaciones militares y en el apoyo que el Estado requiera para anticiparse a la acción de un eventual

adversario que pretenda emplear sus capacidades de ciberguerra de manera ofensiva.

El estudio de la ciberguerra fue abordado por un equipo multidisciplinario de investigadores del CEEAG, quienes seleccionaron y analizaron los planteamientos internacionales referidos al tema, lo que les permitió interiorizarse de los aspectos claves y producir la discusión bibliográfica indispensable para responder a las interrogantes de sus respectivas temáticas, las que son tratadas en la presente publicación.

En la introducción del libro se presenta el planteamiento del problema y el marco teórico referencial de la ciberguerra; en los capítulos que le siguen los lectores podrán familiarizarse con sus antecedentes históricos, con la infraestructura crítica vulnerable a sus efectos, con los lazos que la relacionan con la Disuasión, con el combate por el mando y control al que da origen, con los riesgos y amenazas que representa para la infraestructura crítica, con el Derecho Internacional como marco regulatorio de su accionar y con los desafíos para afrontar la ciberguerra con éxito. El texto concluye con reflexiones finales que sintetizan el conocimiento generado mediante las respuestas a las interrogantes de la investigación pasando a constituirse en los lineamientos para comunicar apropiadamente los resultados obtenidos.

Como Director de la Academia de Guerra me es grato poner a disposición de nuestros alumnos, profesores y de la comunidad académica nacional e internacional el libro *La Ciberguerra: sus impactos y desafíos*, con la seguridad de que contribuye a la formación de los especialistas de Estado Mayor, Ingenieros Politécnicos Militares y a la toma de decisiones por parte de aquellos responsables de conseguir la victoria en el ciberespacio.

Coronel Guillermo Altamirano Campos
Director de la Academia de Guerra del Ejército de Chile

El próximo Pearl Harbor podría llegar vía Internet
Leon Panetta,
Ex-Secretario de Defensa de Estados Unidos

Se buscará sostener que la ciberguerra es un concepto de repercusión estratégica, con un escenario, que es el ciberespacio, que debe ser entendido como una quinta dimensión, lo que es coincidente con la tendencia contemporánea del actuar estratégico.

Introducción

La cibernética, como ciencia asociada a los sistemas de comunicación y de regulación automática de los seres vivos, para su aplicación a sistemas electrónicos y mecánicos que se parecen a ellos, derivó en los tiempos modernos al tema cibernético originado 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. El matemático Norbert Wiener, en la década de los 40, implantó el término inglés *Cybernetics*, orientado a la toma de decisiones, generación de órdenes o simples comandos de acción. En la medida en que se fue haciendo más urgente satisfacer estas demandas se hizo necesario disminuir los tiempos de las etapas de proceso asociado a la información, evidenciando la necesidad de automatizar la mayor cantidad posible de procesos, dando origen a la informática.

La complejidad del tema informático aumentó con la conectividad de computadores y bases de datos, generando la aparición de un espacio virtual o "ciberespacio", como medio de transmisión de datos. Ya no bastaba contar con un computador aislado, sino que su integración a la transferencia de información vino a catalizar notoriamente su importancia como medio informático.

El ciberespacio consiste en una red interdependiente de infraestructuras de tecnologías de la información, incluyendo Internet, redes de telecomunicaciones, sistemas informáticos, procesadores embebidos 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 para la interconexión de sistemas de ordenador mediante Internet.

Siguiendo la definición del DD-10001 Ejército (edición 2017), "el ciberespacio es entendido como el ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior".

Una aproximación conceptual anterior relacionada con la doctrina, el *Ejército y la Fuerza Terrestre*, aportaba que una de las variables que componen el campo de batalla está constituida por el ***ciberespacio***, entendiéndolo como el espacio virtual que contiene los sistemas de redes, las que utilizan medios físicos y el espectro electromagnético para interconectarse y realizar las funciones de procesamiento, almacenamiento y difusión de la información requerida por el sistema de mando y control.

Otra definición, en la línea de lo académico, es entregado por Dan Kuehl, quien indica que: "El ciberespacio es el conjunto de un dominio global dentro del entorno de la información cuyo carácter único y distintivo viene dado por el uso de la electrónica y el espectro electromagnético para crear, almacenar, modificar, intercambiar y explotar información a través de redes interdependientes e interconectadas utilizando las tecnologías de información y comunicaciones".

Entonces, la información es el elemento central para que exista el ciberespacio, por tanto en la actualidad cobra especial importancia el dominio y control de esta dimensión, como también la infraestructura dispuesta para tal efecto, la que es utilizada por diferentes usuarios, como gobiernos, organizaciones y las personas, entre otros. Lo anterior es expresado por la publicación conjunta de Estados Unidos, *Joint Publication 1-02*, que señala que el ciberespacio es "un dominio global dentro del ambiente de la información, consistente en redes interdependientes de infraestructuras informáticas, incluyendo Internet, redes de telecomunicaciones, sistemas computacionales, procesadores y controladores", acepción que es muy similar a la establecida por Luis Feliu, en *Seguridad nacional y Ciberdefensa*, al definirlo como: "un dominio global y dinámico dentro del entorno de la información, compuesto por infraestructura de redes, de tecnología de la información…junto a sus usuarios y operadores".

La concepción de ciberespacio ha ido mutando, convirtiéndose en una conceptualización más amplia, al integrar nuevos elementos como parte de su estructura, inclusive al sumar a la internet como parte de esta, además de definir su alcance como global mediante múltiples conexiones e interdependencias que se derivan, lo que también es incorporado en la Doctrina Nacional de Defensa Conjunta de Chile (DNC): "el ciberespacio

es un dominio global dentro del ambiente informativo, consta de la red de interdependencia de infraestructuras de tecnología de información, incluso Internet, redes de telecomunicaciones, sistemas de computación y controladores y procesadores integrados". Así entonces el ciberespacio constituye un espacio virtual que contiene los sistemas de redes informáticas, los que utilizan medios físicos y el espectro electromagnético para interconectarse y realizar el funcionamiento del procesamiento, almacenamiento y difusión de la información requerida por el sistema de mando y control. Su dominio puede llegar a constituir un factor multiplicador de la fuerza, planteamiento que es muy similar a las definiciones de EE.UU. y España señalados con anterioridad.

Esta publicación, conducida y desarrollada dentro del ámbito investigativo del Centro de Estudios Estratégicos de la Academia de Guerra, ha buscado generar un aporte al área de investigación de ciberguerra, para sobre este tema definir los impactos, transformaciones, estructuras, adaptabilidades o cambios en la infraestructura crítica nacional, proponiendo elementos y acciones que aporten a una estrategia de disuasión en ciberguerra, teniendo a la vista la Política de Defensa, las normativas legales e internacionales, en especial las del derecho internacional de los conflictos armados (DICA).

Así entonces, inicialmente aporta una definición conceptual de la ciberguerra, sus elementos constituyentes y la forma en que se interrelacionan, encadenan y vinculan en sus efectos, particularmente en el ciberespacio asociado a mando y control. Determinado eso, entrega una visión respecto de cuáles entramados de soporte, instalaciones, organizaciones o estamentos, asociados al ciberespacio son considerados infraestructura crítica y cuáles de ellos resultan más vulnerables a la acción de la ciberguerra. Luego se enuncian vulnerabilidades y riesgos de ciberguerra y las subsiguientes amenazas de seguridad, especialmente en lo que comporta el combate por el mando y control, como también sus fortalezas, oportunidades y amenazas, aportando algunas advertencias o soluciones.

El texto no se queda solamente en lo técnico operativo, sino que luego va a la vertiente relacional entre la ciberguerra y su contrastación con la legalidad vigente, nacional e internacional, principalmente en sus relaciones en el ámbito del derecho internacional de los conflictos armados y la conflictividad cibernética.

Se cierra con un análisis basado en las amenazas de ciberguerra identificadas, exponiendo advertencias o soluciones que se pueden sugerir, enunciar o formular a ese respecto, especialmente en lo que comporta el combate por el mando y control, en el contexto de aportar a una estrategia de disuasión.

Definiendo ciberespacio

En la consecuencia del análisis de las variadas y múltiples definiciones de ciberespacio tenidas a la vista, hay elementos comunes que se encuentran en cada una de ellas, resaltando la importancia estructural que dichos conceptos revisten, entre los que destacan "espacio virtual", "datos", "interdependencia e interconexión", "información" e "infraestructura de redes", términos todos que confluyen para un mejor entendimiento de lo que la quinta dimensión viene a significar. Por ello, este ciberespacio va a estar caracterizado por una red de información que lo conforma, donde confluyen redes de tecnología de comunicaciones interconectadas que harán que esa información esté globalmente disponible, usando para ello conexiones físicas e inalámbricas, a altas velocidades.

Algunas de sus características establecidas en el Manual Cybrespace and Electronic Warfare Operations, FM 3-12, son:

Opera en Red

El ciberespacio es una extensa y compleja red global, constituida por medios alámbricos e inalámbricos, conectando nodos que permiten la conectividad de cada dominio. El corazón de esto corresponde a una infraestructura tecnológica, materializada por varios enclaves enlazados a una red con capacidad de data.

Estas redes pueden cruzar fronteras geográficas y políticas, conectando individuos, organizaciones y sistemas alrededor del mundo.

Catalizador Social

El ciberespacio permite la interactividad entre individuos, grupos, organizaciones y Estados-Naciones. Los sistemas computacionales permiten crear, almacenar, procesar, manipular y transportar rápidamente data e información para una selecta o amplia audiencia.

Los usuarios pueden usar esa data para ampliar su ámbito de influencia, cumplir tareas o generar decisiones.

Mensajes de texto, correo electrónico, comercio electrónico, redes sociales y otras formas de comunicación interpersonal selectiva o masiva son posibles gracias al ciberespacio.

Tecnología

Los avances tecnológicos incrementan la complejidad del *hardware* y *software*, requiriendo personal cada vez más capacitado para su gestión. Pero

así como la infraestructura de la red tecnológica y sus capas lógicas son cada vez más complejas, acceder a ellas como usuario se torna cada vez más simple y amigable.

Interdependiente e Interrelacionada

Las operaciones desarrolladas en los otros dominios (tierra, mar, aire, aeroespacio) son dependientes del ciberespacio. Existe una dependencia de la distribución de información y data, la que va directamente ligada a la infraestructura de la red.

Vulnerable

El ciberspacio es vulnerable por varias razones, incluyendo las facilidades de acceso, complejidad del *software* y el *hardware*, actividades inapropiadas. Un individuo o un determinado grupo pueden acceder al ciberespacio en forma simple, solo mediante la disponibilidad de un dispositivo que esté conectado a la red.

Efectos generados en el ciberespacio pueden tener impactos dentro de la dimensión física que ello implica.

Por consiguiente, desde una perspectiva general, las nociones utilizadas permiten reafirmar una tendencia conceptual orientada a establecer que el ciberespacio es parte del escenario donde existen diversos recursos, por este motivo los actores en los que se incluyen a Estados, organizaciones, grupos o individuos competirán por controlarlo y esto generará amenazas y riesgos y, por tanto, una potencialidad de generación de conflictos como parte de una contraposición de intereses.

El ciberespacio fue declarado por *The Economist* y las principales potencias mundiales como el quinto dominio después de la tierra, el mar, el aire y el espacio, debido a que durante la primera década del siglo XXI aparecieron nuevos paradigmas de ataque por medio del ciberespacio, los que basados en diferentes motivaciones individuales o colectivas, intentaban afectar a las instituciones, gobiernos y diversas corporaciones empresariales. Lo expresado es ratificado por Clarke, R. y R. Knake (*Guerra en la red. Los nuevos campos de batalla*, Ariel, 2010) al señalar que: "el ciberspacio es una zona de guerra donde muchas de las batallas del siglo XXI se van a dar", aportando una visualización del ciberespacio como el lugar virtual donde surgirán acciones de amplia variedad y en donde se luchará por ejercer la protección de las redes informáticas.

Por ello podemos aproximar una definición de ciberspacio como "el espacio virtual de carácter global y dinámico dentro del entorno de la infor-

mación donde interactúan los sistemas informáticos, redes e infraestructura asociada más allá de Internet, las que utilizan medios físicos y el espectro electromagnético para interconectarse y realizar las funciones de procesamiento, almacenamiento y difusión de la información, llegando a constituir, junto con otros, una dimensión para controlar y dominar de acuerdo con una política por parte de un Estado o cualquier otra organización".

Desde que Estonia fue víctima de un ataque cibernético a gran escala en 2007, los países se han vuelto vulnerables a ataques de este tipo, porque la sociedad, la economía y la vida cotidiana son cada vez más dependientes del ciberespacio. Así, las amenazas a la seguridad internacional que vemos diariamente están migrando al ciberespacio, por esta razón, se están transformando en un nuevo factor a considerar en lo estratégico.

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. Así, lo concebido inicialmente por Norbert Wiener daba pasos al "control y comunicación en el animal y en la máquina" o "desarrollo de un lenguaje y técnicas que permitieran abordar el problema del control y la comunicación en general".

Capítulo 1

Aparece la ciberguerra

René Leiva Villagra[*]

Introducción

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.

Así, los requerimientos de velocidad en la transmisión y necesidades de almacenamiento de datos fueron en constante 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.

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

* René Leiva es General de Brigada (R) del Ejército de Chile. Oficial de Estado Mayor, 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 en el área de ciberguerra. En el ámbito privado se desempeña como consultor en ciberdefensa para empresas nacionales y extranjeras. rene.leiva@acague.cl, leivarene@yahoo.com

volumétrica, lo que los hacía escasos. Hoy, el vertiginoso avance tecnológico ha transformado los antiguos dinosaurios computacionales en dispositivos que han mutado a aparatos con reducción de sus tamaños y costos, por tanto mucho más masivos, junto con ser diseñados como dispositivos de arquitecturas abiertas, fácilmente portables 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.

Lo anterior incide en tener una percepción de disminución en los niveles de seguridad si los contrastamos con los inicios de la informática, donde los eventos de vulnerabilidad eran menores o casi inexistentes, precisamente porque los computadores eran cajas autárquicas, con circuitos de información cerrados, sin conexión externa, por tanto aislados de amenazas y distantes de los riesgos.

Surge la interrogante de cómo poder definir la ciberguerra, sus componentes conceptuales y constituyentes.

Partiendo por un análisis más detallado de lo antiguo con lo moderno en sistemas computacionales nos lleva a una contrastación de los protocolos de transmisión, verificación, encriptación y proceso, donde se presenta una calidad actual que es exponencialmente superior. Entonces, si las medidas de seguridad presentes son mayores que las del pasado, ¿por qué se da una cantidad mayor de eventos de vulnerabilidad o intrusión informática? La respuesta implica varios factores:

Uno es la cantidad, mucho mayor, de dispositivos computacionales existentes. Como ya se dijo, los antiguos eran muy grandes de tamaño, de alto consumo eléctrico y de alto costo, lo que solo permitía a escasas instituciones y muy pocos privados contar con un ordenador.

En contraste, los nuevos aparatos son de presencia masiva, de costo alcanzable para gran parte de la población, lo que sumado no solamente a computadores, sino que a dispositivos con características informáticas como móviles telefónicos, aparatos "inteligentes", tablets y otros, que hacen mucho mayor el número de elementos conectados a la red.

Sumemos a lo anterior el impacto que ya está teniendo el Internet de las Cosas (IoT, por sus siglas en inglés de Internet of Things), lo que agrega un universo enorme de dispositivos enlazados vía WEB, tanto para actividades domésticas, industriales, comerciales, personales y financieras, entre otras.

Según las estimaciones de Intel, ya hay más de 15.000 millones de dispositivos inteligentes conectados a Internet. Buena parte de estos dispositivos no están lo suficientemente protegidos, como lo afirma el reporte técnico de McAfee Labs[1].

[1] McAfee Labs, *Informe sobre Amenazas*, abril 2017.

La masificación de instrumentos con capacidad computacional o de automatización ha aumentado el universo existente, por esta razón el número de dispositivos que pueden ser víctimas o victimarios es enorme.

Otro factor que ha aumentado el grado de incidencia de los eventos maliciosos es el desarrollo de nuevas formas de optimización de la plataforma de comunicación. Luego, al estar disponible una mayor capacidad de conectividad, las aplicaciones a disposición del usuario han crecido en número y en demanda de ancho de banda (antes no disponible). Por ello, claramente la cantidad de dispositivos móviles con acceso a Internet ha crecido enormemente, superando la de computadores fijos. Junto con ello, la mayoría de estos dispositivos emulan capacidades GPS (localización terrestre), con una tendencia cada vez mayor de contar con LBS (Land Base Systems) que proveen a los usuarios de información en tiempo real, con datos como información de viaje, traslados, navegación, tráfico, meteorología, turismo, ofertas de *retail*, emergencias en la ruta, ayuda en accidentes, pagos en línea, entre muchas otras a nombrar. Eso hace a los usuarios tener una necesidad de permanencia conectados a la *web*, lo que también aumenta los tiempos de riesgo, al estar expuestos permanentemente a amenazas.

La restricción ahora parece haberse volcado más al *hardware*, donde las limitaciones de capacidad de carga de la batería están marcando el límite de la portabilidad a horas de autonomía de energía.

Otro desarrollo va por la vía de los lugares donde se realiza el proceso y el almacenamiento. Cisco estima que para el 2019 los *data centers* "en la nube" van a procesar el 86% de toda la *data* que es necesaria transferir. Esa tendencia es motivada porque los servidores en la nube son dinámicamente escalables en tecnología, tienden a la automatización de muchos de sus procesos de mantención y respaldo. Por ello, muchos *softwares* operan virtualizadamente en la red, sin habitar en el dispositivo usuario, el que va a buscar la aplicación a un servidor en la nube cada vez que la necesite y la va a operar remotamente, con el necesario traspaso de *data* que ese efecto implica. En ese ambiente de nubes, aplicaciones virtuales y flujos de *data* que se conectan por un entramado que no es necesariamente vertical ni jerarquizado, sino que transversal y funcional, corre un estimado de 80% de tráfico, bajo el riesgo de operar en *bypass* de las interfaces de ciberprotección. Acá se remarca el riesgo existente, ya que lo que es una ventaja, la multiconectividad pasa a ser una amenaza al abrir la red a una variedad de dispositivos, aplicaciones, conexiones en la nube, accesos externos dinámicos, todos ellos representando blancos que un ciberagresor va a dimensionar en su valor de disponibilidad de ingresar archivos o programas maliciosos al sistema.

Muchos de estos agentes maliciosos se ocultan en la forma de tráfico de red legítimo o archivos adjuntos, a la vez que explotan funciones de control de

acceso a la red e impactan repetidamente en las corazas que tiene el sistema, explorando y buscando las vulnerabilidades que pueda tener, muchas veces encontrándolas. En ello, lo usual es que los atacantes usen sucesiva o simultáneamente variados medios y vectores de entrada, para asegurar su éxito.

Componentes conceptuales y constituyentes de la ciberguerra

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].

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 guerra[3], desde un punto de vista de la gestión de la información, Boyd 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[4], 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 infoguerra o guerra de la información[5] se ha convertido en una herramienta cada vez más relevante en el desarrollo y consecución de las crisis modernas

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

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

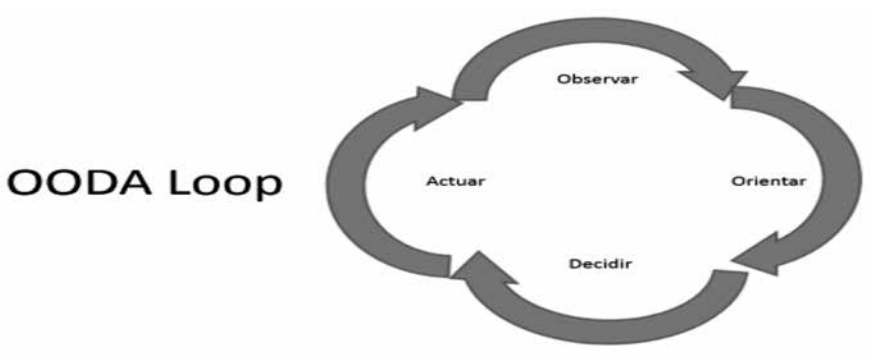
4 John Boid, The School of Advanced Airpower Studies (1997). The Paths of Heaven: The Evolution of Airpower Theory. Air University Press, Maxwell Air Force Base, Alabama, USA. p. 357.

5 Rafael Gomis Pardo y Roberto Plá Aragonés en *El Lado Oscuro de la Era de la Información* definen la Guerra de la Información como "Cualquier acción para denegar, explotar, corromper o destruir la información del enemigo y sus funciones, protegiendo la nuestra contra sus acciones, y explotando nuestras propias operaciones de información".

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 corrupción de los datos"[6]. Es en el ámbito de esta esfera de información donde se constituye un centro de gravedad potencial y relevante, con efectos de la ciberguerra.

Figura 1
Ciclo OODA



Fuente: Elaboración propia.

Al definir la ciberguerra se puede describir como "el uso de capacidades basadas en la red de un Estado, para interrumpir, denegar, degradar, manipular o destruir información residente en computadores y redes de ellos, o los propios ordenadores y las redes de otro Estado"[7].

Si tuviéramos que enumerar las características de una guerra cibernética[8] estas serían: complejidad, asimetría, objetivos limitados, corta duración, menos daños físicos para los soldados, mayor espacio de combate y menor

6 Op. cit. John Boid.
7 Guerra Cibernética, XXXIII Curso de Defensa Nacional, CESEDEN.
8 Gema Sánchez Medero, *Los Estados y la Ciberguerra*, Universidad Complutense de Madrid.

densidad de tropas, lucha intensa por la superioridad de la información, aumenta la integración, mayores exigencias impuestas a los comandantes, nuevos aspectos de la concentración de fuerzas, reacción rápida, e igual de devastadora que una guerra convencional (Thomas, 2001). Pero tal vez, de todas ellas, la más importante sea la de asimetría, porque la guerra cibernética proporciona los instrumentos necesarios para que los más pequeños puedan enfrentarse, incluso vencer y mostrarse superiores a los más grandes, con unos riesgos mínimos para ellos, solo siendo necesario un ordenador y unos avanzados conocimientos informáticos.

La ciberguerra tenderá al logro de objetivos asociados a[9]:

- Dañar un sistema o entidad hasta el punto en que ya no puede funcionar ni ser restaurado a una condición útil sin que lo reconstruyan por completo.
- Interrumpir o romper el flujo de la información.
- Destruir físicamente la información del adversario.
- Reducir la efectividad o eficiencia de los sistemas de comunicación del adversario y sus capacidades de recolección de información.
- Impedir al adversario acceder y utilizar los sistemas y servicios críticos.
- Engañar a los adversarios.
- Lograr acceder a los sistemas del enemigo y robarles información.
- Proteger sus sistemas y restaurar los sistemas atacados.
- Responder rápidamente a los ataques o invasiones del adversario.

Por eso Sánchez Medero nos advierte que existen tres clases de ciberguerra:

Clase I. *Personal Information Warfare*: área relacionada con las cuestiones y la seguridad personal, así como la privacidad de los datos y del acceso a las redes de información.
Clase II. *Corporate/Organizacional Level Information*: área del espionaje clásico entre organizaciones de diferente nivel (de la empresa al Estado) o al mismo nivel (de Estado a Estado).
Clase III, *Open/Global Scope Information Warfare*: área relacionada con las cuestiones de ciberterrorismo a todos los niveles, como pueden ser: los ataques realizados desde computadoras a centros tecnológicos; la propaganda como forma para enviar sus mensajes y para promover el daño ocasionado por sus ataques; o la planificación logística de atentados tradicionales, biológicos o tecnológicos.

9 Ibíd.

Ciberoperaciones

La existencia de ciberoperaciones (COps)[10] corresponde a acciones militares en el ciberespacio, con propósitos de seguridad e inteligencia, constituyendo un instrumento más para la solución de problemas militares en su amplio espectro, dando protección a sistemas y procedimientos vitales para las operaciones propias. Así, las COps son "el empleo de cibercapacidades donde el propósito principal es el logro de objetivos a través del ciberespacio. Estas operaciones incluyen las operaciones en red de computadores y actividades para operar y defender la red de información global"[11].

Estas COps pueden tener un carácter defensivo (ciberoperaciones defensivas, COps-D), o bien un carácter ofensivo (ciberoperaciones ofensivas, COps-O).

En cuanto a la organización de la ciberdefensa, las CNO (Computer Network Operations) se subdividen en tres[12]:

CND (Computer Network Defence), que incluye las acciones para proteger, monitorizar, analizar, detectar, reaccionar y recuperarse frente a los ataques, intrusiones, perturbaciones u otras acciones no autorizadas que podrían comprometer la información y los sistemas que la manejan.
CNE (Computer Network Exploitation), que incluye las acciones de recolección de información para inteligencia acerca de sistemas de información enemigos, así como su explotación.
CNA (Computer Network Attack), que incluye las acciones tomadas para perturbar, denegar, degradar o destruir información que circula por los sistemas enemigos.

Ciberespacio y sistemas de mando y control

Lo que hace complejo de manejar el tema de la ciberguerra es que no corresponde a un término plenamente conceptualizado doctrinariamente, aun cuando hay esfuerzos por aunar consensos en ello[13], pero es un término

10 Ricardo Mesa Illés, *La Ciberguerra: una proposición*, Academia de Guerra, Ejército de Chile, archivo CEEAG, 2016.
11 TRADOC, *Cyberspace Operations Concept Capability Plan 2016-2028*, TRADOC Pamphlet 525-7-8, Ejército de Estados Unidos, Ed. Enero 2010.
12 Joint Chiefs of Staff, *Joint Doctrine for Command and Control Warfare* (C2W), Joint Pub 3-13.1
13 Julio Parra Cereceda, *Aportes a la vinculación del Ciberespacio con los Sistemas de Mando y Control*, octubre 2017.

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 guerra de la información o infoguerra.

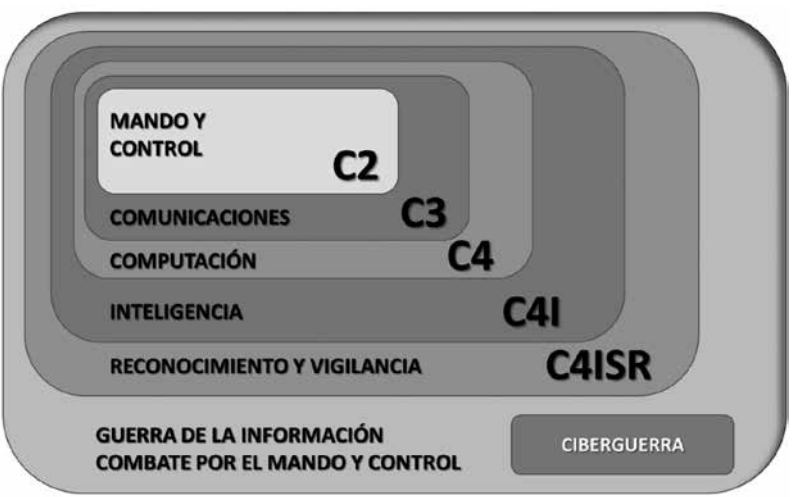
El objetivo principal de la guerra de la información (Information Warfare/ IW) es intervenir en sus fases y procesos, tanto en sus vertientes humanas como automatizadas. Para lograr su cometido IW requerirá importante apoyo de parte de la función inteligencia y de apoyo de telecomunicaciones.

El combate por el mando y control (Command and Control Warfare/ C2W) es una aplicación de IW en operaciones militares y emplea variadas técnicas y tecnologías para atacar o proteger blancos específicos, como también es parte de las IW.

C2W obedece al uso integrado de operaciones psicológicas (PSYOPS), operaciones de decepción, operaciones de seguridad (OPSEC), guerra electrónica (EW) y destrucción física, todo ello apoyado por inteligencia, buscando negar información y así influenciar, degradar o destruir capacidades de C2 adversarias, protegiendo las propias.

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 nuevas herramientas para accionar en el campo de batalla moderno, con un efecto que puede ser transversal a todas sus dimensiones (aire, mar, tierra, espacio más el ciberespacio).

Figura 2
La ciberguerra y su contexto relacional



Fuente: Elaboración propia basado en Joint Pub 3-13.1

Aporta a este encuadramiento conceptual el conjunto de esfuerzos realizados a nivel civil por el Departamento de Seguridad Interna (*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 del mismo país (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*, InfoOps o sencillamente IO")[14].

Ciertamente que como en todo recurso bélico disponible se presentan dos grandes líneas de aplicación medulares: 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.

En lo defensivo se busca proteger el ciberespacio de determinados riesgos y amenazas en beneficio de la seguridad y confiabilidad en su conjunto, dirigido a la protección de la información, sin abandonar un proceso de análisis y gestión de los riesgos relacionados con su uso, como también la detección, seguimiento, bloqueo y neutralización de las amenazas.

Medidas tales[15] como dotarse de medios de seguridad especializados en ciberdefensa para reducir las amenazas y las vulnerabilidades de los mismos, aunque siempre considerando que existe la posibilidad de que sean vulnerados. En este sentido, el intercambio de información entre los actores víctimas de ataques puede ser fundamental, aunque eso siempre es difícil por el miedo que existe a que se filtren datos confidenciales, se conozcan las vulnerabilidades, etc. Otra posible operación es establecer planes de asistencia mutua entre los diferentes componentes de las infraestructuras críticas, de modo que se reduzcan los efectos en cascada debido a su interrelación. Eso sí, todos estos planes deben ser coordinados por un órgano superior a nivel nacional, que debe depender directamente del Departamento Gubernamental encargado de la seguridad del ciberespacio.

También puede aportar el identificar las vulnerabilidades e individualizar los peligros existentes y potenciales que dichas debilidades permiten. Esto solo se puede conseguir con la ciberinteligencia.

El problema que se nos plantea es que Internet carece de fronteras y el contenido ilícito circula de un país a otro en milésimas de segundos, además existe una escasa o nula regulación de los cibercafés, locutorios, salas de informática públicas, bibliotecas, centros educativos, máquinas populares de acceso a Internet y otras donde de forma anónima las personas pueden conectarse y

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

15 Op. cit. Sánchez Medero.

realizar actividades ilícitas. Lo mismo ocurre con las redes inalámbricas libres al alcance de equipos con conexiones capaces de conectarse a esas redes con el anonimato de la no pertenencia al grupo autorizado.

También tiene cabida como posible solución empezar a endurecer la legislación que hace referencia a los delitos informáticos para paliar las posibles deficiencias jurídicas que existen en algunos países. Y otra, como algunos investigadores consideran, es crear una segunda red extraordinariamente controlada y separada del Internet comercial.

En lo ofensivo, son identificables acciones que se ejecutan en el ciberespacio y que permiten la obtención de información mediante virus informáticos que funcionan de la misma forma que un *software* común en cualquier computador o dispositivo, los que hoy son parte de la rutina diaria de cualquier persona. En segunda instancia, el hecho de que estos virus de espionaje obtengan información no solo para generar inteligencia, sino también para programar virus informáticos que ataquen las redes en el ciberespacio y produzcan efectos físicos o ciberlógicos en los sistemas[16].

El impacto de la ciberguerra en la visión estratégica moderna

La ciberguerra es una acción que ha modificado el *locus*, *tempo* y el *pugnator* del conflicto. Fundamentemos por qué ha ocurrido esto:

El *locus* o lugar, porque permite su empleo desde distancias remotas, con una identificación dificultosa de quién la origina y desde dónde, que busca un accionar oculto o clandestino. Para ello encubre el lugar de origen de la acción y va ocultando su huella mediante distintas herramientas tecnológicas que van disipando paso tras paso la ruta eventualmente trazable de su proceder.

El *tempo* también puede tener un momento de ejecución difícil de determinar y detectar, al difuminar su actuar ingresando en sistemas cibernéticos en condición latente o encubierta, para accionar en el momento que sea requerido o teniendo una presencia permanente pero oculta, cual gusano. Para penetrar un sistema explorará permanentemente hasta encontrar agujeros de seguridad en los sistemas operativos, brechas en las aplicaciones, errores en las configuraciones de los sistemas o falta de conocimiento o compromiso de seguridad informática en los usuarios.

16 René Leiva Ureta, *Estrategias de Ciberseguridad en el Mundo y su Contribución a una Estrategia de Ciberseguridad Nacional*, octubre 2015, ANEPE.

Esta búsqueda puede ser previo, durante e incluso postconflicto y tiende a ser una actividad continua de monitoreo "defensivo".

Los diferentes actores preparan desde tiempos de paz el campo de batalla cibernético. Todos ellos buscan las vulnerabilidades del adversario, y se esfuerzan por infiltrarse en sus sistemas y plagarlos de "bombas lógicas" y detectar "puertas traseras", para poder utilizarlas cuando se inicien las hostilidades. Esto termina desvaneciendo la línea divisoria entre el tiempo de guerra y el de paz, lo que dificulta el poder catalogar la conducta de los contendientes y denunciar a un actor cuando esté quebrantando la paz y la seguridad internacionales[17].

También ha variado el ***pugnator*** porque 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. En ello identificamos blancos de infraestructura crítica, cubriendo todos los ámbitos de acción, afectando la población civil y los servicios que requiere para subsistir.

Es tal el impacto de la ciberguerra en la definición de estrategias[18], que en el caso de EE.UU., entre el 2009 y 2010, el Subsecretario de Defensa William J. Lynn conceptualizó cinco principios básicos de la estrategia de la guerra del futuro:

- En lo relativo a la guerra, el ciberespacio debe ser reconocido como un territorio de dominio igual que la tierra, el mar y aire.
- Cualquier posición defensiva debe ir "más allá" del mero mantenimiento del ciberespacio "limpio de enemigos" para incluir operaciones sofisticadas y precisas que permitan una reacción inmediata.
- La defensa del ciberespacio debe ir más allá del mundo de las redes militares y dominios .gov y .mil del Departamento de Defensa para llegar hasta las redes comerciales y que deben estar subordinados al concepto de Seguridad Nacional.

17 Manuel Ricardo Torres Soriano, "Los Dilemas Estratégicos de la Ciberguerra", *Revista Ejército*, España, Nº 839, marzo 2011, pp. 14-19.

18 Op. cit. Mesa Illés, CEEAG, 2016.

- La estrategia de defensa ciberespacial se debe realizar con los aliados internacionales para una política efectiva de alerta compartida ante las amenazas mediante el establecimiento de ciberdefensas con países aliados.
- El Departamento de Defensa debe contribuir a mantener e incrementar el dominio tecnológico de Estados Unidos y mejorar el proceso de adquisiciones y mantenerse al día con la agilidad que evoluciona la industria de las tecnologías de la información (TICs).

Ha aumentado considerablemente nuestra dependencia de las plataformas digitales, por lo que su disponibilidad y accesibilidad se vuelven recursos críticos. Nos vemos enfrentados a nuevos riesgos y amenazas, cada vez más sofisticados y dinámicos, que pueden afectar la confidencialidad y la integridad de la información que circula por nuestras redes. Lo anterior ha obligado a adoptar medidas en el gobierno que sirvan para gestionar y enfrentar estos riesgos, no solamente a nivel público, sino también en coordinación con el sector privado, la academia y la sociedad civil[19].

Por ello, las ciberredes han ido tomando mayor connotación en el tiempo, ya no solo siendo una plataforma de transporte de información, sino que pasando a constituir brazos remotos que comandan, gestionan, monitorean, activan y conectan gran parte de los recursos tecnológicos de que disponemos, constituyendo en sí infraestructuras que por su importancia pasan a ser críticas.

El ciberespacio no está libre de amenazas y agresiones. La Red de Conectividad del Estado, por dar un ejemplo concreto de Chile, registró un aumento en los patrones maliciosos que la afectan de más de cien millones de ataques, entre 2014 y 2015, pasando el 2016 a cifras exponencialmente más altas por ataques de Denegación Distribuida de Servicios (DDoS)[20]. De ahí la importancia que el sistema sea concebido y mantenido con una condición robusta, que asegure, sino total, al menos parcialmente, un rango de servicios de conectividad y transferencia de *data* que sea útil, suficiente e incorruptible.

19 Marcos Robledo Hoecker, Subsecretario de Defensa, *Discurso Seminario Ciberseguridad*, Facultad de Derecho de la Universidad de Chile 27/11/2015.

20 Mahmud Aleuy Peña y Lillo, Subsecretario del Interior, Presidente, Comité Interministerial sobre Ciberseguridad, Política nacional de Ciberseguridad (PNCS 2017), p. 7.

Sistema informático

En este punto es necesario recordar cuáles son los componentes de un sistema informático y sus subsistemas, para, a partir de ellos, desprender los objetivos que pueden ser rentables para la aplicación de una ciberagresión.

Un sistema informático es definido[21] como la organización, obtención, proceso, transmisión y diseminación de información, de acuerdo con procesos definidos, tanto manuales como automáticos. En un concepto mayor de guerra de la información, esto considera la estructura total, su organización y componentes que permiten la búsqueda, proceso, archivo, transmisión, proyección y difusión de información.

En una conformación básica, un sistema informático está compuesto por los siguientes componentes[22]:

Aplicaciones del usuario (Word, correo electrónico, procesos utilitarios, planillas electrónicas, etc.).
Aplicaciones de producción, proceso o específicas (Enterprise Resource Planning/ERP, Instagram, Project, Facebook, Spotify, etc.).
Aplicaciones de infraestructura (telecomunicaciones, conmutación, registros, etc.).
Protocolos de interconexión (TCP/IP, IPX, DECnet, AppleTalk, XNS, OSI, X.25 etc.).
Sistemas operativos (Linux, Windows, Unix, MVS, VMS, etc.)
Hardware (procesadores, canales de comunicación, medios de archivo, otros).

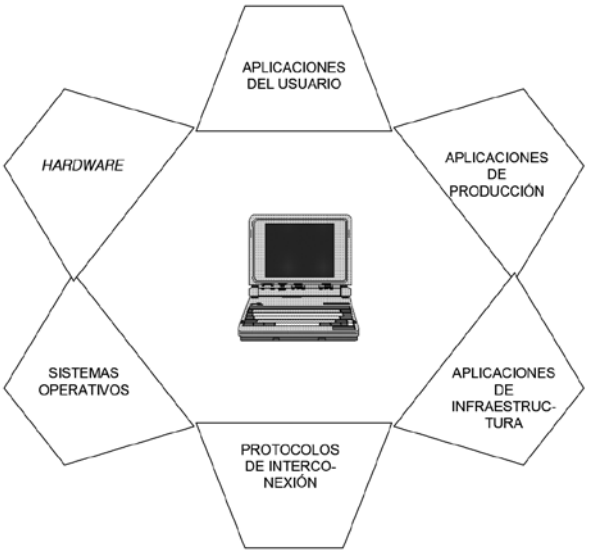
Cada uno de estos componentes se interrelacionan y conforman varios subsistemas, los que dependerán del proceso que se esté apoyando[23]:

Subsistema de procesamiento de datos

Todos los elementos orientados a tratar los datos y someterlos a algún tipo especial de tratamiento con el que se espera obtener algún resultado. Intervienen dispositivos de *hardware* y aplicaciones de *software*.

21 Department of Defense, *Joint Force Employment Considerations*, Appendix A, Joint Electronic Library, Estados Unidos de América, Ed. Feb. 2000.
22 Kent Anderson, *Intelligence-Based Threat Assesment for Information Networks and Infraestructures*, Global Tech Reserach Inc., marzo 1998, p. 7.
23 Héctor Gómez Arriagada, *Definición de Subsistemas*, Respuesta a Entrevista.

Figura 3
Esquema de conformación básica de un sistema informático



(Elaboración propia).

Subsistema de almacenamiento de datos

Medios de almacenamiento de los datos. Su propósito es proveer la cantidad suficiente de capacidad de almacenamiento, de manera de tener los datos a disposición de los usuarios.

Subsistema de transmisión de datos

Mecanismos de traspaso de los datos desde un dispositivo a otro.

Subsistema de seguridad de datos

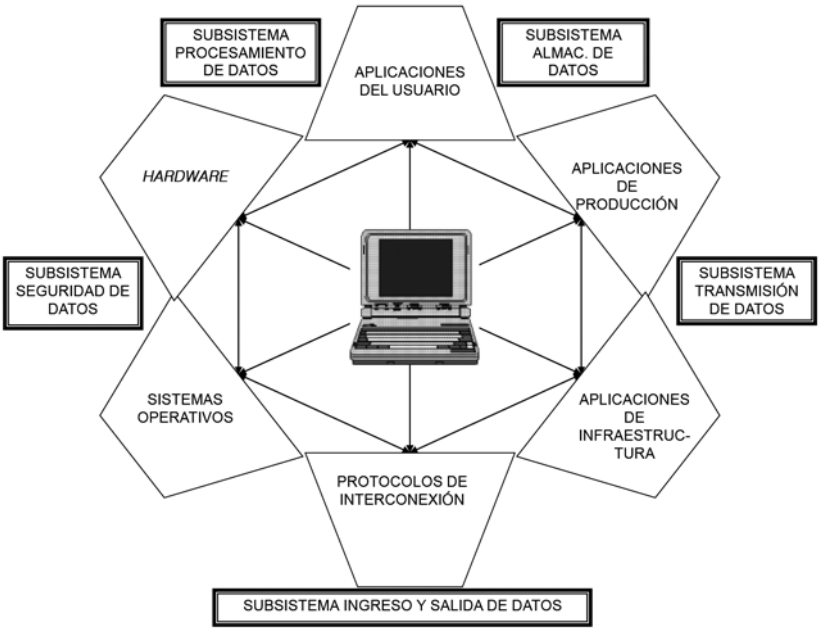
Mecanismos de *hardware*, *software* y administrativos, cuyo propósito es mantener la seguridad de datos desde el punto de vista de la integridad, confidencialidad y disponibilidad.

Subsistema de ingreso y salida de datos

Todos los dispositivos utilizados para ingresar o extraer datos desde un sistema informático.

Figura 4

Esquema de subsistemas de un sistema informático



(Elaboración propia).

Los sistemas de información son una parte de una infraestructura mayor de información, a la que se le asignan tres tipos de categorías conocidas como:

Infraestructura de información global

Corresponden a redes de comunicaciones, computadores, bases de datos y servidores electrónicos que generan vastas transferencias de información, la que está disponible para sus usuarios. Su cobertura es a nivel mundial. Internet es el mejor ejemplo para ello.

Infraestructuras de información a nivel nacional

Su definición se acerca a la anterior, variando su grado de cobertura, la que es limitada a un nivel nacional. Ejemplos de lo anterior corresponderían a la Red de Conectividad del Estado (RCE), la Red de Emergencia del Ministerio del Interior, la red de control del Sistema Interconectado Central (electricidad), Redbank, entre otros.

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 acerca del concepto de ciberguerra, que sigue los lineamientos de ser una herramienta más en una estrategia de acción[24]. Ejemplos de sabotaje de Israel a la capacidad nuclear de Irak, espionaje de países orientales a otras potencias, son presentados como herramientas usando los medios respecto de la plataforma de la ciberguerra.

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 pueden ser una amenaza para las grandes potencias, forjándose y desarrollándose el concepto de las operaciones militares centradas en redes[25]. En los conflictos tradicionales normales 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[26].

En lo anterior no se debe caer en la confusión que la ciberguerra, por actuar en un ciberespacio, se enmarca en una forma no territorial de la guerra irregular[27], pues aun cuando las ciberagresiones se darán en una dimensión virtual, sus efectos buscados serán circunscritos a un espacio real del adversario, con efectos concretos que afecten su potencialidad. Es más, al analizar los límites de este espacio virtual, conformado y entendido como una nueva dimensión del campo de batalla, se pueden distinguir tres áreas: una física, una lógica y una organizacional.

El área física es aquella en que los límites pueden ser reconocidos legalmente (*de jure*), así como podrían ser los límites entre dos países, o por vía de la praxis (*de facto*) como podría ser la línea de faja (AOR) entre dos unidades distintas. Por ello, lo físico es complejo de definir en lo virtual.

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

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

26 Op. cit. Pastor Acosta, Pérez Rodríguez y otros, ISDEFE-UPM.

27 Op. cit. Hervé Coutau-Bégarie, *Tratado de Estrategia.*

El área lógica está delimitada por el diseño de las diferentes capas de la red observada. Estas capas representan la independencia física y lógica de los componentes de *software* en función de la naturaleza de los servicios que proporcionan.

El área organizacional tiene una connotación más bien funcional para su delimitación, por ejemplo si es dedicada al área comercial, investigativa, científica, energética, defensa, policial, etcétera.

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 su continuidad histórica[28]. En lo que se refiere a la ocupación del territorio adquiere dos formas complementarias entre sí: la *ocupación física* y la *ocupación funcional*[29]. 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 las de otros Estados mediante la fijación de unas fronteras (terrestres, aéreas y, en su caso, marítimas) que deben controlarse y defenderse de manera permanente como requisito necesario para garantizar su seguridad. Pero esto, se plantea, tiene una extensión a los espacios que siendo de la jurisdicción el Estado/Nación trascienden de lo físico y subsisten en lo virtual, donde claramente el ciberespacio tiene cabida como territorio virtual, por ello 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.

Aunque los principios de la estrategia, basados en la naturaleza humana, no cambiarán, el análisis estratégico debe tener en cuenta la quinta dimensión y su capacidad de reducir drásticamente la fricción, lo que exigirá repensar las reglas y los modelos de gobernanza del mundo en su totalidad[30].

Respecto de la estrategia típica de un ciberataque en esta quinta dimensión, la mayoría de las intrusiones aprovechan las vulnerabilidades de los

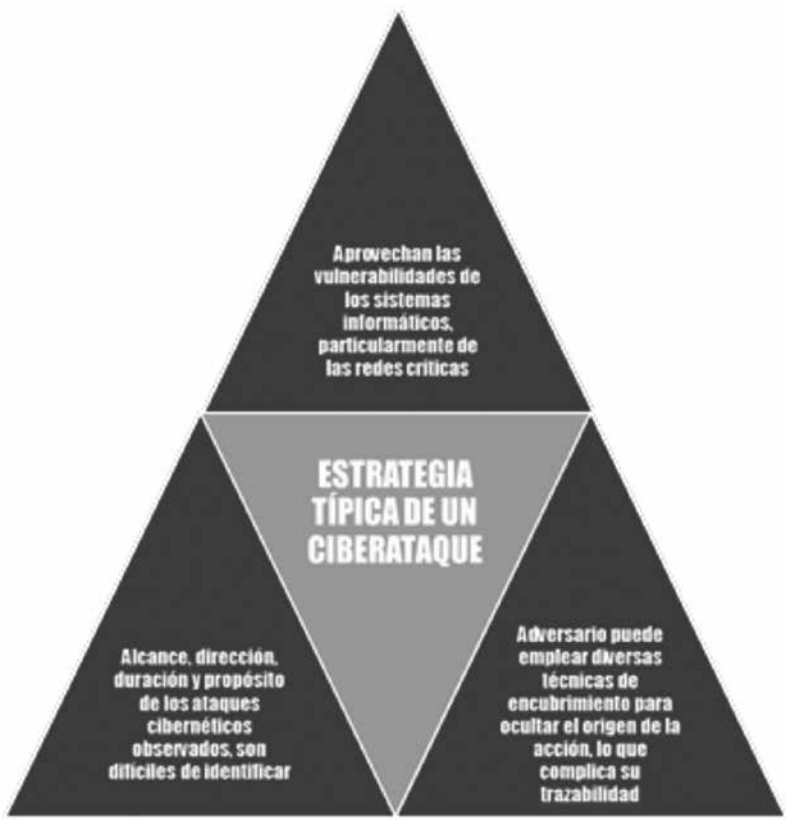
28 Rafael Calduch Cervera, *La Ocupación del Territorio Nacional y la Disuasión para su Defensa: La Cambiante Perspectiva Europea*, Universidad Complutense de Madrid.

29 Ibíd.

30 José María Fuster van Bendegem, *La quinta dimensión digital*, Instituto Español de Investigaciones Estratégicas, disponible http://www.ieee.es/Galerias/fichero/docs_marco/2016/DIEEEM19-2016_Quinta_Dimensioxn_Fuster.pdf

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 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[31].

Figura 5
Estrategia típica de un ciberataque



Fuente: Elaboración propia.

31 Op. cit. Luis Saez Collantes.

Reflexiones finales

En la modificación del *locus*, *tempo* y el *pugnator* del conflicto hay una relación compleja entre Estados y *hackers*, ya que no siempre el Estado será responsable de las acciones de ciberguerra llevadas a cabo por sus ciudadanos o incluso por extranjeros que ciberoperen dentro de su territorio. Se trata de un asunto extremadamente tortuoso. En ocasiones, el Estado no solo carece de control sobre estos grupos, sino que también es víctima de sus acciones. Esta cuestión se complica aún más como consecuencia de las dinámicas de actuación de los *hackers*, los que engloban a multitud de individuos que actúan simultáneamente desde diferentes países, y bajo diferentes jurisdicciones.

Entonces, habiendo descrito los actores que operan en determinados sistemas (ya también enunciados), podemos representar que esto ha traído impactos en lo conceptualizado de la estrategia como irregularidad[32], porque la vertiente jurídica de la guerra en su *jus ad bellum* (derecho a la guerra) deberá ampliar en su análisis los actores que tienen participación en la legítima defensa, junto con su criterio fundamental de actuación basado en la soberanía, ya que el "quinto dominio" corresponderá a una conformación virtual y no territorial.

También en lo propio del *jus in bellum* (derecho en la guerra) se presenta una articulación nueva, distinta, innovadora, porque deberán evaluarse las reglas de conducta, reglas de enfrentamiento, particularmente en su proporcionalidad, necesidad e inminencia, que será iluminada por el efecto que determinadas acciones cibernéticas puedan alcanzar y lo dinámico que la ciberguerra comporta.

En esta ciberguerra se busca irrumpir o destruir, a lo menos, los sistemas de mando, 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 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, etc. Podrá considerar el cegamiento electrónico, la perturbación (*jamming*), decepción, la intrusión en los sistemas de información y comunicaciones adversarios, entre otros.

[32] Hervé Coutau-Bégarie, *Tratado de Estrategia*, pp. 209-211, Colección Academia de Guerra del Ejército de Chile.

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[33].

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.

Se debe tener una visión amplia al enfrentar esta compleja temática de ciberamenazas, la que no debe ir solo por un vector de atención de entidades policiales que deben cuidar plataformas complementarias que pueda usar el terrorismo, es tener una visión muy focalizada del amplio campo en que este factor puede incidir.

Bibliografía

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.

Anderson, Kent. *Intelligence-Based Threat Assesment for Information Networks and Infraestructures*, Global Tech Reserach Inc., marzo 1998.

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

[33] 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.

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).

Department of Defense. *Joint Force Employment Considerations*, Appendix A, Joint Electronic Library, Estados Unidos de América, Ed. Feb. 2000.

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

Fuster van Bendegem, José María. *La quinta dimensión digital*, Instituto Español de Investigaciones Estratégicas, disponible http://www.ieee.es/Galerias/fichero/docs_marco/2016/DIEEEM19-2016_Quinta_Dimensioxn_Fuster.pdf

Gomis Pardo, Rafael y Plá Aragonés Roberto. El Lado Oscuro de la Era de la Información, Revista Aeronáutica y Astronáutica Nº 672, abril 1998.

Guerra Cibernética. XXXIII Curso de Defensa Nacional, CESEDEN.

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

Leiva Ureta, René. *Estrategias de Ciberseguridad en el Mundo y su Contribución a una Estrategia de Ciberseguridad Nacional*, octubre 2015, ANEPE.

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.

Mesa Illés, Ricardo. *La Ciberguerra: una proposición, Academia de Guerra, Ejército de Chile, archivo CEEAG*, 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.

Torres Soriano, Manuel Ricardo. "Los Dilemas Estratégicos de la Ciberguerra", *Revista Ejército*, España, Nº 839, marzo 2011.

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.

Capítulo 2

Infraestructura crítica vulnerable a la ciberguerra

Hernán Díaz Mardones[*]

Introducción

Las ventajas y oportunidades que hoy se presentan con los avances en los ámbitos de la informática y de las telecomunicaciones, conocidas como TIC (tecnologías de la información y comunicación), permiten el acceso, producción, comunicación, integración y trabajo de información bajo diferentes formas o códigos, como imágenes, textos, sonido, etc., constituyendo la Internet una red global de comunicaciones interconectadas que permite una conectividad integral. Es posible señalar que ya han pasado más de veinte años desde el surgimiento de la Internet, después de su origen militar en EE.UU., oportunidad en la que se dio un gran salto cualitativo, que cambió y redefinió los modos de conocer y relacionarse del hombre. A lo anterior, y en forma inseparable, se suma el desarrollo de los computadores y *software*, junto con los aparatos móviles de comunicaciones de grandes capacidades, siendo estos últimos en la actualidad los principales medios por los que se accede a la Internet.

Este desarrollo tecnológico ha traído consigo acceso a grandes cantidades de *data*, transmisión de archivos, correos electrónicos, mensajería instantánea, etc., incluyendo el acceso a información general, privada, incluso de tipo

* Hernán Díaz Mardones es Coronel (r) del Ejército de Chile. Master of Business Administration, MBA in International Business, Universidad Gabriela Mistral; Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile; Ingeniero Comercial, mención en marketing, UDLA; Oficial de Estado Mayor del Ejército de Chile y de la Fuerza Aérea de Chile, Certificado en MBTI-Myers and Briggs Type Indicator, otorgado por HDS, México. hdiazm@acague.cl

personal, lo que facilita y simplifica la vida tanto en los ámbitos personal como profesional. De esta forma, todas las organizaciones, públicas como privadas, empresas, servicios de diferentes tipos, industrias, etc., han tomado como una de sus principales herramientas el uso de la Internet para mejorar y hacer más eficientes sus propias funciones, optimizando sus propios recursos y a la vez obtener las retribuciones económicas que traen consigo. Para facilitar o gestionar lo anterior, se han creado sistemas de redes, almacenamiento y distribución de megadatos, comunicaciones y otra variedad de infraestructuras que dan sustento al "negocio" de cada una de estas organizaciones en pos de sus fines.

Pero así como se facilita y se hace más expedito todo nuestro quehacer, también se hace más vulnerable, surgiendo riesgos que pueden llegar a convertirse en serias amenazas, afectando particularmente los servicios, organizaciones y estructuras que tienen un rol vital en el desarrollo de las actividades esenciales del ser humano del mundo moderno, las que en particular se denominan infraestructuras críticas (IC), cuyo daño o afección puede tener graves efectos en los intereses esenciales y la seguridad de cualquier país. Estos riesgos provienen de múltiples fuentes y se manifiestan mediante actividades de espionaje, sabotaje, fraudes o ciberataques realizados por otros países, por grupos organizados o por particulares, entre otros, surgiendo las denominadas ciberamenazas.

De ahí es que resulta imprescindible el crear soluciones para prevenir y controlar esos posibles riesgos y amenazas que implica el uso del ciberespacio, cuyo empleo con fines de causar daño a las IC pudiese efectuarse mediante una expresión extrema con la ciberguerra.

En ese contexto, resulta necesario establecer la relación entre la ciberguerra y las infraestructuras críticas, visualizando cuáles de estas pueden tener una mayor vulnerabilidad a las acciones de la ciberguerra, tomando como referencia a los principales actores del mundo en el tema, como lo son Estados Unidos y Europa, particularmente el caso de España y las acciones que han establecido para enfrentar este fenómeno. A su vez, realizar una aproximación a los roles que cumplen en esta relación las entidades públicas y privadas y las necesidades que surgen de ello.

Antecedentes y el conocimiento existente

La preocupación por la protección de la infraestructura crítica en muchos países se refleja mediante programas, planes, medidas legislativas, etc., tal es el ejemplo de los programas y acciones presentados por los presidentes Bill Clinton, George W. Bush y Barack Obama. Por su parte, el rey Juan Carlos I

de España promulga el 2011 la Ley de Protección de Infraestructuras Críticas (Ley PIC 8/2011), complementada por el Real Decreto 704/2011. Todos ellos con el claro fin de protegerlas, junto con sus activos claves de alto valor, que pueden convertirse en objetivos para sus adversarios potenciales.

Los aspectos claves en la formulación de una eventual estrategia de ciberguerra y la normativa para el uso de las armas cibernéticas son un tema que requiere análisis e investigación debido al escaso conocimiento y experiencia existente al respecto, donde se destaca el aporte documental de los conflictos cibernéticos entre naciones y el Manual de Derecho Internacional de Tallin (Tallinn Manual on the International Law Applicable to Cyber Warfare).

Este manual[1] fue publicado en el 2013 por el Centro de Excelencia para la Ciberdefensa Cooperativa de OTAN (CCD COE), que se aboca a un tópico emergente a nivel mundial, por lo que todo lo relacionado con el ciberespacio seguirá cambiando, aumentando su importancia y junto con ello la necesidad para las definiciones y desarrollo de normas. Es en ese contexto, pareciera ser, que surge la pregunta acerca de la importancia de contar con una estrategia global en el tema de la seguridad cibernética, lo que se comprueba con el debate que han comenzado de los aspectos jurídicos por Estados Unidos, las Naciones Unidas, la Organización del Tratado del Atlántico Norte y la Unión Europea, como respuesta al creciente problema de los ataques cibernéticos, la ausencia de políticas adecuadas y aspectos de orden legal[2].

Definiendo la infraestructura crítica

Cada Estado define y determina lo que constituye su infraestructura crítica, algunos autores definen la infraestructura crítica como "las capacidades básicas, los sistemas técnicos y las organizaciones responsables de la provisión de activos"[3]. La Comisión Europea define la infraestructura crítica como un "activo o sistema que es esencial para el mantenimiento de las funciones vitales de la sociedad"[4].

La ya citada Ley de Protección de Infraestructuras Críticas de España define como infraestructuras críticas aquellas "cuyo funcionamiento es

1 Documento que examina cómo poder aplicar las normas existentes de derecho internacional a la nueva Ciberguerra.

2 Thomas A. Johnson, *Cyber-Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare,* Boca Raton; Florida EE.UU., CRC Press Taylor & Francis Group, 2015, preface.

3 Emery Roe and Paul R. Schulman, *Reliability and Risk: The Challenge of Managing Interconnected Infraestructures*, California, Standford University Press, 2016.

4 European Commission, Critical Infraestructure (2013). Bajo: https://ec.europa.eu/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure_en (Jun 12 2017).

indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales para el desarrollo normal de las actividades y la vida de las personas". En ese contexto, los servicios esenciales se constituyen como aquellos necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas. Por otra parte, también se define como infraestructuras estratégicas a las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información en las que descansa el funcionamiento de los servicios esenciales[5], generándose una interrelación entre las organizaciones que cumplen una determinada función calificada como esencial y el sistema tecnológico que la soporta y hace posible acceder a ellas.

Lo que es común en todas las definiciones es lo referido a los componentes de la infraestructura crítica, que puede incluir comunicaciones, servicios de emergencia, energía, represas, finanzas, alimentos, servicios públicos, industria, salud, transporte, gas, comunicaciones públicas, radio y televisión, tecnologías de la información, instalaciones comerciales, sector químico y nuclear, y agua. Muchos países dependen cada vez más de la infraestructura crítica, particularmente por los servicios que prestan, actividades y funciones que en general desarrollan, cuya afectación tiene importantes consecuencias y en las que tienen poco o ningún control, ya que normalmente se encuentran parcial o totalmente fuera de su jurisdicción.

Lo anterior se debe a que la infraestructura crítica en su gran mayoría es propiedad del sector privado, estimándose que más del 80 por ciento de ella en los países occidentales es operada y de propiedad de dicho sector[6]. En consecuencia, dondequiera que se encuentre la mencionada infraestructura, el Estado puede no estar en condiciones de garantizar la seguridad integral de ellas y puede depender en gran parte de las medidas, acciones e inversiones del sector privado para este fin. De ello surge como lógico que una alianza estratégica entre los sectores público y privado sea fundamental para una política de protección de la infraestructura crítica.

5 Boletín Oficial del Estado de España Nº 102, *Ley de Protección de Infraestructuras Críticas PIC 8/2011, Real Decreto 704/2011*, 29 de abril 2011, p. 4.

6 United Nations Security Council, Counter-Terrorism Committee, Executive Directorate, *Physical protection of Critical Infrastructure against terrorist attacks, CTDE Trends Report*, 8 marzo 2017, p. 2.

Algunos antecedentes de la infraestructura crítica en Estados Unidos y Europa

La Directiva de Política Presidencial de EE.UU., PPD-21, se orienta a mejorar y fortalecer los esfuerzos para mantener y asegurar las infraestructuras críticas. En esa misma directiva se reconoce que ella es diversa y compleja, incluyendo la distribución de sus redes, las diferentes estructuras organizacionales y los diferentes modelos operativos que funcionan tanto en el espacio físico como en el ciberespacio, siendo estas gubernamentales, privadas o multinacionales.

En esta Directiva presidencial, EE.UU. declara que su infraestructura crítica debe ser segura, capaz de resistir y recuperarse rápidamente de los peligros y amenazas, para ello deben proveerse de prevención, protección, mitigación, respuesta y recuperación, mediante planes y programas para reducir las vulnerabilidades, minimizar las consecuencias, identificar e interrumpir las amenazas e incrementar los esfuerzos de respuesta y recuperación de esta. Para lo anterior se le asigna la responsabilidad al Secretario del Departamento de Seguridad Nacional para promover la seguridad y resiliencia de las infraestructuras críticas del país. En función de ello debe identificar y priorizar las vulnerabilidades tanto físicas como las cibernéticas, en coordinación con las demás agencias sectoriales. En el mismo contexto, se le dispone mantener dos centros nacionales de infraestructura crítica, los que son operados por el departamento de Seguridad Nacional, uno para la infraestructura física y otro para la infraestructura cibernética, funcionando ambos en forma integrada[7].

Además, asigna la responsabilidad del desarrollo de la Fuerza de Tarea Conjunta Nacional de Investigación Cibernética (NCIJTF), operada por el FBI, con el objeto de coordinar, integrar y compartir información pertinente relacionada con ciberamenazas. Este equipo tiene representación del Departamento de Seguridad Nacional, la comunidad de inteligencia, el Departamento de Defensa y otras agencias, según corresponda; el Procurador General y el Secretario del Departamento de Seguridad Nacional colaborarán para llevar a cabo sus respectivas misiones de infraestructura crítica. La directiva presidencial incluye en materia de investigación y desarrollo (I+D) las actividades financiadas con fondos federales que buscan fortalecer la seguridad y la resistencia de la infraestructura crítica del país.

7 EE.UU., Presidential Policy Directive (PPD-21) on Critical Infrastructure Security and Resilience, Feb. 12, 2013.

La directiva presidencial, PPD-21, identificó los siguientes 16 sectores de infraestructura crítica y las Agencias del Sector Específico (SSAs, Sector Specific Agencies) a cargo de cada una de ellas:

1. Química: SSA: Departamento de Seguridad Nacional.
2. Instalaciones comerciales: SSA: Department of Homeland Security.
3. Comunicaciones: SSA: Departamento de Seguridad Nacional.
4. Fabricación Crítica (Critical Manufacturing): SSA: Departamento de Seguridad Nacional.
5. Represas: SSA: Departamento de Seguridad Nacional.
6. Defensa Industrial Base: SSA: Departamento de Defensa.
7. Servicios de Emergencia: SSA: Department of Homeland Security.
8. Energía: SSA: Departamento de Energía.
9. Servicios Financieros: SSA: Departamento de Hacienda.
10. Alimentación y Agricultura: Co-SSAs: Departamento de Agricultura de los Estados Unidos y Departamento de Salud y Servicios Humanos.
11. Instalaciones gubernamentales: Co-SSAs: Departamento de Seguridad Nacional y Administración de Servicios Generales.
12. Salud y Salud Pública: SSA: Departamento de Salud y Servicios Humanos.
13. Tecnología de la Información: SSA: Department of Homeland Security.
14. Reactores nucleares, materiales y desechos: SSA: Department of Homeland Security.
15. Sistemas de Transporte: Co-SSAs: Departamento de Seguridad Nacional y Departamento de Transporte.
16. Sistemas de agua y alcantarillado: SSA: Agencia de Protección Ambiental.

Las 16 infraestructuras críticas mencionadas, por una parte, son para EE.UU. la base de lo que han convertido a dicho país en una potencia mundial, pero también pasan a constituir vulnerabilidades si se convierten en blanco de un ataque. Al analizarlas se puede establecer que no todas las 16 infraestructuras críticas definidas en esta directiva presidencial son vulnerables a un ataque cibernético; sin embargo, las que efectivamente lo son forman parte de los recursos más críticos de esa nación.

En Europa, gran parte de los países de la Unión Europea han elaborado una Estrategia Nacional de Seguridad Cibernética, documento clave que incluye las medidas que se deben adoptar para hacer frente a los riesgos cibernéticos. Cada país tiene un enfoque propio respecto del tema, el que es diverso y de acuerdo con sus requerimientos nacionales, es decir, algunos países han desarrollado Planes de Acción Específicos, otros han creado grupos de trabajo por sector crítico para enfocarse en la protección de la

infraestructura crítica de la información y en el organismo responsable de la ciberseguridad nacional[8].

Desde el 2012 la European Union Agency for Network and Information Security (ENISA) ha estado apoyando a los países miembros, siendo su punto de partida en ello la realización de un balance de las actividades de ciberseguridad en Europa, analizando las tendencias y entregando recomendaciones para que los países diseñen, apliquen y evalúen una estrategia. El objetivo de esas estrategias nacionales de seguridad cibernética es garantizar que los Estados miembros estén preparados para afrontar riesgos graves, sean conscientes de sus consecuencias y prestos para responder adecuadamente. Sin embargo, se señala que existen inconvenientes en cuanto a las capacidades nacionales de coordinación en casos de incidentes transfronterizos y en términos de participación y preparación del sector privado. Basado en ello es que la Estrategia de Seguridad Cibernética de la UE de 2013 (EUCSS) pide a ENISA que "fomente las buenas prácticas en materia de seguridad de la información y de las redes para asistir y apoyar a los Estados miembros en el desarrollo de capacidades nacionales de ciberseguridad y la infraestructura energética"[9].

Por su parte España, como se mencionó, publica en abril del 2011 la Ley 8/2011, Protección de la Infraestructura Crítica (Ley PIC), definiendo las infraestructuras críticas, estableciendo cuáles servicios la conforman y los sistemas, tecnología y redes que las soportan, calificándolas como estratégicas[10].

Los dos grandes objetivos de esta norma son: 1) Catalogar el conjunto de infraestructuras que prestan servicios esenciales a nuestra sociedad, y 2) Diseñar un planeamiento que contenga medidas de prevención y protección eficaces contra las posibles amenazas hacia tales infraestructuras, tanto en el plano de la seguridad física como en el de la seguridad de las tecnologías de la información y las comunicaciones.

Respecto de la protección de las infraestructuras críticas, la Ley 8/2011 la define como el conjunto de actividades destinadas a asegurar la funcionalidad, continuidad e integridad de las infraestructuras críticas con el fin de prevenir, paliar y neutralizar el daño causado por un ataque deliberado contra dichas infraestructuras y a garantizar la integración de estas actuaciones con las demás que procedan de otros sujetos responsables dentro del

8 European Union Agency for Network and Information Security (ENISA), Critical *Information Infrastructures Protection approaches in EU*, 2015, pp. 1-3.

9 Jefatura de Estado "BOE (Boletín Oficial del Estado)", Nº 102 de 29 de abril 2011, referencia: BOE-A-2011-7630, "Medidas de Protección de Infraestructuras Críticas", España (29 abril 2011).

10 Jefatura de Estado "BOE", Nº 102, 2011.

ámbito de su respectiva competencia. De igual modo, esta ley ha establecido las siguientes infraestructuras críticas: administración, agua, alimentación, energía, espacio, industria química, industria nuclear, instalaciones de investigación, salud, sistema financiero y tributario, tecnologías de la información y las comunicaciones y transportes.

Se puede deducir que los principales aportes de esta ley son la creación del Sistema Nacional de Protección de Infraestructuras Críticas, establecer las bases para el Sistema de Planificación PIC, generar el Catálogo Nacional de Infraestructuras Estratégicas y establecer el CERT (Equipo de Respuesta ante Emergencias Informáticas, del inglés Computer Emergency Response Team) para la gestión de incidentes de ciberseguridad.

Al respecto, se visualiza que una política que incluya la ciberseguridad de infraestructuras críticas deberá contener un esquema acabado de áreas, funciones y entidades estatales responsables que servirán para identificar y delimitar el nivel de impacto de cada sector. Además, deberá señalar qué órganos técnicos serán los encargados de ejecutar las medidas que se deriven de esa política, considerando aquellos estándares especiales de ciberseguridad, atendiendo a los particulares niveles de madurez de las IC, especialmente respecto de sus procesos esenciales. En este sentido, se aprecia que las seleccionadas como las más relevantes en EE.UU. son aquellas catalogadas como las más críticas sobre la base de su impacto de interdependencia con las otras definidas como tales, estas son: energía y la red eléctrica, transportes y telecomunicaciones[11]. Por su parte, España tiene similitud en sus propias IC, siendo la del "espacio" la única diferente a las especificadas por EE.UU., pero en general están contenidas tanto por uno como por otros en sus respectivas leyes o políticas.

La ciberguerra y la infraestructura crítica

En el nivel estratégico y con relación a la afectación de las infraestructuras críticas ya mencionadas anteriormente, se asigna como la primera ciberguerra al conflicto de la Estonia rusa el 2007, debido al ataque masivo denominado ataque distribuido de denegación de servicio (distributed denial-of-service (DDoS) en contra de Estonia. El motivo de asignar a este evento como la primera guerra cibernética o ciberguerra se debe al compromiso real de la Organización del Tratado del Atlántico Norte (OTAN) en el establecimiento de un Centro de Defensa Cibernética en el 2008 en Tallin, Estonia. Otra razón

11 Thomas A. Johnson, 2015, p. 43.

está en el hecho de que este fue el ataque DDoS más grande jamás visto, con más de un millón de computadoras dirigidas a las infraestructuras críticas del área de la economía, el comercio y las comunicaciones de Estonia a nivel nacional. Ello se tradujo en que los usuarios estonios no pudieron usar sus tarjetas de crédito, realizar operaciones bancarias, recibir noticias y comunicarse mediante los canales normales de comunicación. Este ataque duró semanas y obligó a Estonia a considerarlo como un acto de guerra, y como miembro de la OTAN, solicitaron ayuda al Consejo del Atlántico Norte de la Alianza Militar de la Organización. El hecho que la OTAN estableciera un Centro de Defensa Cibernética en Tallin se marca como un hito al ser la primera vez que se adopta esta acción; por otra parte, los expertos en ciberseguridad rastrearon la actividad cibernética estableciendo que estaban bajo el control de Rusia, sin embargo, este lo negó declarando que falsificaron sus sitios[12].

Un ataque distribuido de denegación de servicio (DDoS) es un ataque en el que múltiples sistemas informáticos comprometidos atacan a un objetivo, como un servidor, un sitio *web* u otro recurso de red y causan una denegación del servicio para los usuarios del recurso de destino. Su principal característica es la inundación de mensajes entrantes, solicitudes de conexión o paquetes con malformaciones dirigidos al sistema de destino, lo que obliga a disminuir la velocidad o incluso a bloquearse y apagarse, negando así el servicio del sistema a los usuarios legítimos[13]. Por otra parte, los paquetes con malformaciones (malformed packets) se refieren a cualquier ataque que utiliza paquetes no estándar para causar denegación de servicio, estos ataques generalmente explotan errores en el protocolo de control de transmisión y protocolo de internet (TCP / IP) inundando el sistema de la víctima mediante el envío de paquetes con formato atípico[14].

A nivel de empleo de las fuerzas, uno de los hechos que dan cuenta de los comienzos de la ciberguerra ocurrió en 1990 y 1991, en circunstancias que EE.UU. enfrentaba a Irak en la denominada "primera guerra del Golfo", ocasión en la que cinco piratas informáticos de origen holandés penetraron en sistemas informáticos de 34 sitios militares norteamericanos por medio de Internet. De este hecho se obtuvo información de la planificación militar de EE.UU. para la Operación Tormenta del Desierto, dentro de la que se encontraban detalles acerca de la ubicación exacta de tropas, armas y movimiento de buques de guerra en la región del golfo. Estos antecedentes se

12 Thomas A. Johnson, 2015, pp. 177-178.

13 Search Security Techtarget, "Distributed denial of service (DDoS) attack", 2017. goo.gl/k7217h (consultado 14 de junio 2017).

14 Ebscohost Connection, "Malformed Packet Attack", marzo 2007. goo.gl/bQtgan (consultado 14 de junio 2017).

traspasaron a las autoridades iraquíes, pero estos la desecharon por estimar que se trataba de información falsa, y que formaba parte de una operación de decepción o engaño, lo que en realidad no fue así[15].

Por otra parte, dentro de las operaciones en el contexto de la ciberguerra, en la misma Guerra del Golfo mencionada anteriormente está el hecho del desarrollo de operaciones ofensivas por parte de EE.UU. Un ejemplo de ello es la realizada al inicio de este conflicto y que precedió a la invasión por las fuerzas de la coalición, que tuvo como resultado dejar fuera de servicio la mitad de los sistemas computacionales de las fuerzas militares de Irak, lo anterior se realizó mediante la instalación de virus en dispositivos (*hadware*) en Francia y enviados a Irak por intermedio de Jordania, los que estaban diseñados para desactivar las computadoras Windows y el computador central[16].

Otro hecho importante de destacar en relación con la ciberguerra y los efectos de esta en las infraestructuras críticas, es el caso de China. Después de las guerras del Golfo, con las experiencias y aprendizajes derivados de ese conflicto, China efectuó un cambio significativo dando un paso trascendente en el desempeño de sus medios militares y de las acciones relacionadas con la ciberguerra, ello después de observar al ejército iraquí enfrentar a EE.UU. y sus aliados utilizando sistemas de armas soviéticos y chinos, similares a los usados por sus propias fuerzas, con los que fueron derrotados en 42 días debido a la tecnología avanzada y a la estrategia de guerra de información de EE.UU. Con esta experiencia llegaron a la conclusión de que la guerra tradicional se cambiaría para siempre debido al uso de sistemas de información y tecnología avanzada y a la integración de estos, definiéndolos como fundamentales para los cambios y avances necesarios para un nuevo y moderno ejército chino[17]. Con esas nuevas características, la nueva doctrina china se enfocaría a las capacidades de tipo ofensiva y dirigida a la infraestructura del enemigo, así como la infraestructura bancaria, los sistemas de redes eléctricas y otras infraestructuras críticas, centrándose en los aspectos de la fuente de poder de una sociedad determinada, que inevitablemente son los sistemas económicos y los sistemas esenciales, con el fin de debilitar a la nación enemiga hasta el punto de que la guerra regular entre militares no sería necesaria[18].

El actual grado de capacidades chinas para desarrollar acciones de ciberguerra, según EE.UU., se sostiene en el robo de propiedad intelectual de corporaciones norteamericanas, laboratorios de investigación, contratistas de

15 Thomas A. Johnson, 2015, p. 156.
16 Thomas A. Johnson, 2015, p. 156.
17 Thomas A. Johnson, 2015, p. 179.
18 Jennifer Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press), 2005.

defensa y los propios militares, obteniéndolas mediante el ciberespionaje. Según investigaciones, se han obtenido por ese medio cientos de datos e informaciones de 141 organizaciones y compañías que involucran a 20 industrias importantes, mediante ataques que se centran no en hacer daño, sino en la exfiltración de datos y permanecer ocultos en los sistemas de información de la organización objetivo durante el mayor tiempo posible. Dentro de las revelaciones conocidas, existen algunos diseños de armas obtenidos por las mencionadas actividades de ciberespionaje de China, entre ellas destacan los diseños para el sistema avanzado Patriot Missile-Pac-3, el terminal High Altitude Defense para disparar misiles, Aegis de la Armada sistema de defensa de misiles balísticos, el avión de combate F/A-18, el helicóptero Black Hawk, el nuevo buque de combate del litoral de la marina y el F-35 Joint Strike Fighter. La obtención ilegal de estos diseños de sistemas de armas representa miles de millones de dólares de ventajas de combate para China y un ahorro para ellos de al menos 25 años de investigación y desarrollo. El 2014 el Departamento de Justicia norteamericano reunió pruebas suficientes para acusar a cinco grandes entidades chinas de múltiples cargos de espionaje cibernético ilegal[19].

Teniendo consideración de lo anterior, se puede establecer que existe una clara y directa relación entre la ciberguerra y las infraestructuras críticas, ello debido a que las últimas pasan a conformar objetivos, mediante estos, quien quiera afectar una determinada área esencial de una nación, lo puede lograr mediante la anulación, interrupción, destrucción de una determinada IC.

Como nota interesante derivada de los antecedentes descritos está la importancia que el Teniente General Adjunto Qi Jianguo atribuye a la toma y el mantenimiento de la superioridad en el ciberespacio, porque cree que hoy apoderarse del ciberespacio es más importante que el dominio del espacio marítimo y del aire, que en su momento lo tuvo durante la Segunda Guerra Mundial.

Reflexiones finales

Las acciones ofensivas en una ciberguerra se pueden lanzar virtualmente desde cualquier rincón del mundo, por cualquier país, organización o incluso individuos, razón por la que la necesidad de crear estrategias de defensa para proteger las infraestructuras críticas es más que fundamental. Sin lugar a dudas, considerando las diferentes estrategias, políticas y acciones

19 Thomas A. Johnson, 2015, pp. 179-183.

que diferentes países se han propuesto con ese fin, el diseño, preparación e implementación de estrategias defensivas que tengan como punto de partida la prevención, advertencias de intrusión y detección, disuasión, y otros mecanismos de defensa, son fundamentales para evitar vulnerabilidades y adelantarse a las amenazas. Enseguida, algunas medidas relacionadas a ataques de características contraofensivas como parte de la estrategia defensiva, constituirán el siguiente paso y dependerá en gran medida del desarrollo tecnológico asociado a las capacidades que las infraestructuras críticas, tanto de origen privado como públicas, sean capaces de integrar, teniendo cubierto de la mejor manera posible sus medidas defensivas como base para este desarrollo.

Las infraestructuras críticas, como ya se mencionó en los diferentes países tomados como ejemplo, son definidas en forma general como instalaciones, redes, servicios y equipos físicos y de tecnología de la información, siendo un aspecto relevante el que sean consideradas estratégicas, por estar relacionadas con la provisión de bienes y prestación de servicios públicos esenciales y cuya afectación pudiera comprometer la Seguridad Nacional. Sin embargo, resulta importante la definición de detalle de cada una de las IC, con el fin de desarrollar las estrategias de protección y la ciberdefensa de sus componentes. Entre ellas y de acuerdo con las experiencias de los principales países expuestos, en Chile se pueden desde ya considerar diferentes áreas, entre las que se encuentran las empresas que manejan las aguas, como presas, tratamiento y redes de distribución; otras en centrales de energía eléctrica; del sector salud, incluyendo hospitales; las relacionadas con el transporte, entre ellas los aeropuertos, terminales de autobuses; las relacionadas con la industria química, incluyendo el transporte de elementos de alto riesgo como materiales químicos, biológicos y radiológicos; también el sistema financiero, incluyendo en este los bancos, bolsas de valores, recaudación de impuestos, etcétera.

Con ese fin, lo planteado por la directiva presidencial de EE.UU., PPD-21, en relación con las capacidades que deben desarrollar las IC: "ser segura, capaz de resistir y recuperarse rápidamente de los peligros y amenazas, para ello deben proveerse de prevención, protección, mitigación, respuesta y recuperación, mediante planes y programas para reducir las vulnerabilidades, minimizar las consecuencias, identificar e interrumpir las amenazas e incrementar los esfuerzos de respuesta y recuperación", resultan, bajo las experiencias descritas, de la mayor relevancia, resultando más que conveniente que el trabajo que se genere de cualquier país para la promulgación de una política o estrategia nacional de ciberseguridad, relacionado con las políticas específicas de ciberdefensa, las tengan en consideración.

Como se deduce, en las diferentes áreas que pueden integrar las IC se encuentran involucrados organismos y entidades, pertenecientes al sector

público y privado, por tanto resulta importante establecer la necesidad de que ambas áreas del quehacer estén integradas y coordinadas para que los efectos de las diferentes estrategias sean los apropiados y exitosos, ya sea mediante alianzas estratégicas entre ambos sectores, la colaboración formal e informal entre ellos, las asociaciones público-privadas, en algunos casos mediante procedimientos legales, con el fin de asegurar que las partes interesadas participen en la protección de las IC, todas estas estrategias, acciones o medidas deberán amoldarse a las diferentes IC en particular, ya que resulta poco probable que un modelo único sea aplicable a diferentes entidades.

Además, del hecho mismo de la necesidad de integración y coordinación, otro aspecto importante de incluir en los análisis para los efectos antes mencionados, es la conformación por sobre las diferentes IC de un ente integrador y coordinador, que permita un adecuado cumplimiento de funciones, intercambio de información, adopción de estrategias, difundir experiencias, mejora de capacidades, capacitación y estudio del panorama internacional y ataques ocurridos a las IC en diferentes lugares del mundo para que junto con tomar conciencia ayude a diseñar proyectos de protección, normativa, etc. En ese contexto, la educación continua de todos los integrantes componentes de una IC acerca de las ciberamenazas y las prácticas de seguridad fundamentales, son esenciales para ayudar a reducir el riesgo de error y para fortalecer las áreas de colaboración. En síntesis, una arquitectura de carácter integral en seguridad que actúe sobre las funciones de protección, detección y mejora continua, mejorando la gestión de los riesgos, la combinación y fortalecimiento de nuevas herramientas.

Como se puede deducir, la relación de la ciberguerra con las infraestructuras críticas es de carácter directo, ya que constituyen los objetivos reales mediante los cuales quien quiera ejercer efectos nocivos en una determinada área de las que componen dichas infraestructuras, pueden paralizar una nación por un tiempo determinado, logrando aprovechar las vulnerabilidades mediante ataques desde cualquier parte del mundo. Estas acciones y efectos pueden darse en diferentes niveles, siendo lo normal por las experiencias descritas que sucedan en niveles de orden nacional.

Respecto de las que tengan mayor vulnerabilidad a las acciones de la ciberguerra, se puede afirmar que están en general aquellas relacionadas con las instalaciones, redes, servicios y equipos físicos, todos ellos asociados y sustentados en la tecnología de la información, particularmente con acceso a Internet, destacando principalmente las relacionadas con energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, protección civil y defensa, siendo característico su consideración como estratégicas, por su relación con las actividades esenciales y prestación

de servicios públicos fundamentales y cuyas consecuencias pudiera comprometer la Seguridad Nacional.

Bibliografía

Council of the European Union. "Identification and designation of European critical infrastructures and the assessment of the need to improve their protection", *Official Journal of the European Union*, Nº 114/EC (diciembre 2008).

Ebscohost Connection. "Malformed Packet Attack" (marzo 2007).

Edgar Vásquez Cruz. "Proteger la infraestructura crítica, una tarea fundamental en ciberseguridad nacional", McAfee Securing Tomorrow (Documento en línea, 6 de junio 2016) (https://securingtomorrow.mcafee.com/author/edgar-vasquez-cruz/). [Consultado 19 de julio 2017].

Emery Roe and Paul R. Schulman. *Reliability and Risk: The Challenge of Managing Interconnected Infraestructures*, California: Standford University Press, 2016.

European Union. "Critical Information Infrastructures Protection approaches in EU", Agency for Network and Information Security (ENISA), 2015.

Gobierno de España. "Ley de Protección de Infraestructuras Críticas PIC 8/2011", Boletín Oficial del Estado de España Nº 102, Real Decreto 704/2011, 29 de abril 2011.

http://connection.ebscohost.com/c/reference-entries/31667776/malformed-packet-attack (Documento en línea) [consultado 14 de junio 2017].

http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF (Documento en línea) [consultado el 18 de junio 2017].

Jennifer Sims and Burton Gerber. *Transforming U.S. Intelligence,* Washington: Georgetown University Press), 2005.

Johnson, Thomas A. *Ciber-Security: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare*, Boca Raton, Florida: CRC Press, Taylor & Francis Group, 2015.

Jorge Kamlofsky, Hugo Colombo, Matías Sliafertas, Juan Pedernera. *"Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas"*, CAETI - Universidad Abierta Interamericana, Buenos Aires, Argentina, noviembre 2015.

Manuel Sánchez. "*Infraestructuras Críticas y Ciberseguridad"*, Director para Europa de la World Security Federation (WSF), julio 2011.

Search Security Techtarget. "Distributed denial of service (DDoS) attack" (2017), http://searchsecurity.techtarget.com/definition/distributed-denial-of-service-attack (Documento en línea) [consultado 14 de junio 2017].

U.S. Government. Presidential Policy Directive (PPD-21) "On Critical Infrastructure Security and Resilience", EE.UU., Feb. 12, 2013.

United Nations Security Council. "Physical protection of Critical Infrastructure against terrorist attacks", CTDE Trends Report, Counter-Terrorism Committee, Executive Directorate, 8 marzo 2017.

Capítulo 3

La lógica de la ciberguerra y su relación compleja con la disuasión

René Leiva Villagra[*]

Introducción

En la línea de seguir desarrollando la visualización de impactos de la ciberguerra, caemos en la disuasión, como elemento constitutivo de la estrategia moderna, donde nos indica Torres Soriano que se considera que todos los actores estatales tratan de disuadir a sus potenciales enemigos desarrollando capacidades de respuesta que les permitan sobrevivir y responder militarmente a una agresión previa. Así, por ejemplo, la capacidad de infligir un daño similar o mayor al sufrido neutralizaba el atractivo que algunos contendientes podían encontrar en lanzar un primer ataque.

Este convencimiento fue la base sobre la que, durante décadas, se construyó la estrategia nuclear y que hizo posible que ninguno de los países dotados de estas armas decidiese recurrir a ellas contra otro actor nuclear. Sin embargo, para que dicho equilibro disuasorio sea posible no solo es necesario poseer los medios para el ataque, sino también ser vulnerable a la represalia del enemigo.

* René Leiva es General de Brigada (R) del Ejército de Chile. Oficial de Estado Mayor, 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 en el área de ciberguerra. En el ámbito privado se desempeña como consultor en ciberdefensa para empresas nacionales y extranjeras. rene.leiva@acague.cl; leivarene@yahoo.com

Por ello, ir a una respuesta de la interrogante de cómo se relaciona la ciberguerra con la disuasión pasa a ser una necesidad como aporte al pensamiento estratégico. Acá, como buscará demostrarse, existe una línea relacionada entre estos elementos, que pasa por la vía del entendimiento de las amenazas, para de esa forma ir conjugando ideas de acción respecto de la base del concepto de articular el arte de la estrategia con la tecnología de lo cibernético y sus consideraciones que para con el área de defensa implica.

Es aquí[1] donde empiezan a surgir los problemas cuando hablamos de ciberguerra. Por ello, en el ámbito estratégico surge la pregunta de cómo generar disuasión en el ciberespacio, donde la sorpresa y el secreto son claves, pero donde el requerimiento de exteriorizar en forma creíble y real esa capacidad se da como una situación necesaria y funcional, como factor previo imprescindible al efecto de *deterrence*.

Las ciberarmas son dispositivos de un solo uso, continúa Torres Soriano. La posibilidad de infiltrarse y desbaratar la infraestructura informática del adversario descansa generalmente en el descubrimiento de vulnerabilidades en el diseño de sus sistemas y el *software* que lo mantiene activo. Su utilidad depende directamente de que el potencial atacado desconozca la existencia de estas brechas en su seguridad. Queda, por tanto, descartada la posibilidad de que un actor estatal decidiese hacer una demostración de sus capacidades de ciberguerra con una finalidad exclusivamente disuasoria.

La implementación de un pequeño ataque deja tras de sí un rastro digital, que puede ser estudiado y que permite crear los parches para evitar un nuevo ataque utilizando el mismo procedimiento. De igual modo, las ciberarmas tienen una caducidad muy rápida. Las vulnerabilidades en los sistemas enemigos desaparecen como consecuencia de la continua evolución tecnológica y de programación de unos sistemas en continua actualización.

Hacia una disuasión ciberaplicable

La teoría de la disuasión se basaba en una aplicación creíble y lograble de represalia, que buscaba prevenir que el oponente ataque, porque de hacerlo recibiría castigo por una acción ofensiva que lo destruiría o al menos le generaría un enorme daño.

Esto le plantea a los ciberguerreros el dilema de si deben hacer uso de esta ventaja sobre su adversario antes de que esta desaparezca, sobre todo,

[1] Manuel Ricardo Torres Soriano, *Los Dilemas Estratégicos de la Ciberguerra*, Revista Ejército, España, Nº 839, marzo 2011, pp. 14-19.

si no existe la seguridad de que en el futuro vuelva a poseer esta ventana de oportunidad.

El carácter necesariamente secreto de estas armas, junto con su atractivo para actores incapaces de desafiar convencionalmente a sus adversarios, hace tremendamente difícil que se pueda alcanzar un tratado de control y limitación de ciberarmas. De hecho, la lógica de la ciberguerra no solo hace compleja la disuasión, sino que también beneficia al contendiente que decide tomar la iniciativa y lanzar el primer ataque. El tiempo transcurrido entre la decisión de llevar a cabo el ataque y sus efectos es prácticamente imperceptible, lo que dificulta la existencia de un sistema de alerta temprana y anticipación. Esto crea un entorno estratégico tremendamente inestable, con una elevada posibilidad de iniciar un ciberconflicto como consecuencia de un error, una mala interpretación de las acciones del adversario, o una incorrecta atribución de responsabilidades.

Al analizar la teoría de la disuasión, que en su conjunto estableció el fundamento de las relaciones y estrategias que dieron forma a la Guerra Fría, en esencia se está frente a una capacidad de represalia creíble que puede impedir que los adversarios ataquen, ya que saben que si lo hacen serán destruidos. En ello, Howard define la estrategia de la disuasión como el intento de persuadir a un adversario por medio de la amenaza de una represión, implicando que los costes (para el agresor) de utilizar la fuerza militar para resolver un conflicto político sobrepasarán los beneficios que pudieran obtenerse[2]. En la actualidad se tiende a aplicar la disuasión clásica a la esfera cibernética[3], pero hay mucha confusión acerca de cómo la disuasión funcionaría en ese dominio.

El ámbito de acción de la disuasión no es una panacea y no impide totalmente que adversarios cibernéticos penetren en nuestras redes e infraestructuras. El éxito de la disuasión se reduce a nuestra capacidad de convencer a los adversarios que sus intrusiones cibernéticas implicarán un costo demasiado alto para ellos, pero cuando los objetivos que nos pueden ser batidos son de un alto valor y el agresor no posee mucho que perder, la ecuación costo-beneficio se torna muy favorable para el atacante y le da una condición asimétrica crítica, generando un atractivo índice neto de rentabilidad.

En la llamada guerra asimétrica se miden bandos con fuerzas muy dispares. Es claro que, debido al carácter mortífero del conflicto armado, cada parte buscará la máxima superioridad o asimetría. Más que un término asociado a la desigualdad, o a la incapacidad de un bando débil frente a uno de fuerzas

2 M. Howard Reasurance and Deterrence, *Western Defense in the 1980's*, Foreign Affaires, 61 (winter 1982-1983), p. 315.

3 Rhea Siers, *Mitos de la Ciber Disuasión*, The Cipherbrief.

abrumadoras, la opción asimétrica busca la conformación de desequilibrios mediante recursos que exceden lo convencional e incluso llegan a lo clandestino. Por ello, un enfrentamiento asimétrico[4] a lo que hace referencia es a batallas que tienen lugar entre fuerzas disimilares que utilizan determinados factores o estrategias para alterar el escenario del enfrentamiento y así obtener una ventaja sobre el oponente. Esos factores pueden ser el engaño, la sorpresa, la velocidad, el movimiento, el uso de armas de forma inesperada.

La ventaja (y la voluntad de aprovecharla) es lo que permite a un ejército prevalecer sobre otro. La guerra asimétrica es también un medio con que fuerzas militares inferiores ganan ventaja sobre oponentes más poderosos, o al menos con más recursos. Términos como "no tradicional" o "no convencional" son también utilizados a la hora de definir la guerra asimétrica porque en esta se emplean métodos que no encajan con las imágenes más extendidas de la guerra. También puede ser entendido como guerra asimétrica el uso de nueva tecnología con que una fuerza militar superior derrota a otra fuerza militar inferior. Todos estos elementos podrían combinarse para conseguir una completa definición de la guerra de este tipo (asimétrica), pero tal vez lo más relevante es que lo asimétrico abarcaría todo aquello que altera el campo de batalla, de tal manera que se niega la ventaja del oponente.

El problema fundamental para la Defensa es el cambio que las nuevas tecnologías han producido. Si en el pasado era suficiente con aprovecharse de las nuevas capacidades de los sistemas de información y del ciberespacio para mejorar la eficacia operacional de las Fuerzas Armadas, ahora es necesario poder combatir, y ganar, en el ciberespacio.

La Defensa requiere asegurar las capacidades en el ciberespacio para poder garantizar la efectividad en las operaciones tradicionales. Se ha dicho del ciberespacio que es el campo de batalla del futuro. Este cambio obliga a modificar los conceptos y doctrinas que se aplican a la confrontación clásica, que deben ser adaptados a las exigencias de un escenario virtual. Este proceso adaptativo debe ser el punto de partida para la definición sólida y la creación ordenada de una capacidad de ciberdefensa.

La protección y la defensa del ciberespacio se han convertido en uno de los retos fundamentales para las Fuerzas Armadas de la mayoría de los países, de ahí la necesidad de disponer de ellas adaptadas a un entorno con continuos avances tecnológicos y dentro de un presupuesto cada vez más restrictivo. El riesgo omnipresente de ataques desde el ciberespacio hace prever que en los futuros conflictos las primeras acciones tengan lugar en el ciberespacio.

[4] César Pintado Rodríguez, *De la Guerra (Asimétrica)*, Boletín 55/2014, 19 mayo de 2014, Instituto Español de Estudios Estratégicos.

En lo anterior, el efecto de la ciberguerra tiene una potencialidad de aplicación enorme. A causa de que la ciberguerra va a operar en un escenario de dimensión distinta, que es el ciberespacio, como entorno virtual que contiene los sistemas de redes informáticas, donde se utilizan medios físicos y el espectro electromagnético para interconectarse y realizar el funcionamiento del procesamiento, almacenamiento y difusión de la información requerida por el Sistema de Mando y Control, su dominio puede llegar a constituir un factor multiplicador de las fuerzas, por tanto será un factor que coadyuvará en la concreción del anhelado desequilibrio.

Existen actores en el ciberespacio que poseen capacidad técnica para provocar muchos estragos en un amplio espectro[5]. Muy pocos pueden hacer mucho daño y, por tanto, la ciberguerra es el paradigma de la guerra asimétrica. Cubeiro considera también que, en este ámbito, el esfuerzo del defensor es mayor que el que pueda realizar el agresor. La ciberdefensa es mucho más cara y compleja que el ciberataque. Además, cuanto más técnico-dependiente es una nación, una organización o un ejército, más vulnerables serán a este tipo de agresiones. Más adelante, aseguró que existe un considerable vacío legal en el ciberespacio. Esta ausencia de autoridad favorece al agresor y hace que la trazabilidad del ataque y su origen sean muy difíciles de controlar.

Las fuerzas convencionales, al ser enfrentadas a este tipo de conflicto asimétrico, requieren necesariamente una reconfiguración de sus estructuras, procedimientos, entrenamiento e incluso equipamiento. Por lógica ese tipo de fuerzas estarán conformadas para actuar contra ejércitos de características similares, regulares y convencionales. Al ser el escenario enrarecido por un accionar de medios opositores que agreden desde una dimensión distinta, como lo es el ciberespacio, una fuerza convencional, por grande que sea, podrá hacer poco o nada ante ello. Esto implica que la capacidad de ciberguerra, en sus componentes defensivos, ofensivos y exploratorios, debe ser desarrollada, mantenida y sostenida con antelación, porque de no hacerlo se estará en riesgo real y concreto de ser víctima del desequilibrio que el conflicto asimétrico busque.

Desde que Estonia fue víctima de un ataque cibernético a gran escala en 2007, los países se han vuelto vulnerables a ataques de este tipo, porque la sociedad, la economía y la vida cotidiana son cada vez más dependientes del

5 Enrique Cubeiro, Capitán de Navío, Jefe de Operaciones del Mando Conjunto de Ciberdefensa, *Conciencia nacional de ciberdefensa*, Centro Superior Estudios de la Defensa Nacional (CESEDEN), Jornadas Construyendo la Ciberdefensa en España, http://www.defensa.gob.es/Galerias/gabinete/red/2014/red-306-ciberdefensa.pdf

ciberespacio. Las complejidades y amenazas a la seguridad internacional que vemos diariamente están inmigrando al ciberespacio[6].

Volvemos entonces a la teoría de la disuasión, que sintéticamente es la degradación de una intención agresora sobre la base de la amenaza e imposición de un castigo, lo que opera a lo largo de un conjunto continuo.

Esta relación de poderes opera sobre una base en que es necesaria una línea lógica, donde la racionalidad está presente, donde hay intereses definidos y principales. En ello entonces se actúa para sacar el máximo provecho y reducir al mínimo las posibles consecuencias negativas[7].

Esta teoría entonces depende en buena parte de actores que evalúan las consecuencias a favor y en contra, basándose en la consideración de las acciones y reacciones posibles de cada uno.

La complejidad en ello aparece cuando la racionalidad está ausente y toma protagonismo el arrebato o la intención de daño en ausencia de fortaleza o estructura crítica propia que pueda ser afectada, permitiendo al agresor ser aún más arriesgado en su operación. El ciberterrorismo, usado en la crisis o en el conflicto, como herramienta de ciberguerra será un ejemplo de ello. También lo será el uso de ciberagresión en guerra asimétrica, donde logra una alta relación en la ecuación de beneficio para el que es más débil. Así definido ello, si el agresor tiene poco (como reducidas infraestructura crítica dependiente del ciberespacio, por ejemplo), arriesga poco al ofender, pero es atraído e impulsado a ello por el daño que puede inferir, junto con la dificultad eventual en ser identificado como fuente de la acción agresiva.

Por ello la disuasión nuclear no aplica necesariamente como un referente para la estrategia de ciberguerra. Hay ciertas diferencias significativas entre el poder nuclear y cibernético. Por ejemplo, el "club" cibernético es mucho más amplio que el club nuclear, además de contener un sinnúmero de actores que no son estatales, englobando el ámbito privado, académico, industrial, comercial e incluso individual. Muchos actores, de diferente raigambre, están permanentemente en la línea de defensa contra intrusiones y ataques cibernéticos. Por ello, la disuasión cibernética necesariamente debe contener en su estrategia una respuesta multiparticipativa privada-pública.

Parte de la disuasión será basada en la resiliencia de la red cibernética. Para ello se debe ser capaz de demostrar que hay procesos y recursos para responder a los ataques cibernéticos y contener las interrupciones, con

6 Edgardo Riveros, Subsecretario de Relaciones Exteriores, Seminario Internacional "Ciberseguridad y Ciberdefensa en Chile", 27 de noviembre de 2015, Aula Magna, Facultad de Derecho, Universidad de Chile.

7 Alan Dershowitz, *Por qué aumenta el Terrorismo*, Ediciones Encuentro, Madrid.

respaldos versátiles y robustos, para así desalentar a algunos actores si creen que sus acciones serán menos impactantes de lo previsto.

Las demás condiciones, componentes o requisitos de la disuasión dependen del disuasor. Es pues su responsabilidad que la disuasión funcione. Es decir, que exista. Pues hablar de fallos de la disuasión no es más que una manera impropia de expresarse. Si se produce la agresión es que no se cumplía alguna de las condiciones que crean la disuasión. Entre estas podemos identificar una de carácter físico y varias de carácter psicológico, ya que la disuasión es ante todo un fenómeno psicológico La disuasión está en la mente del disuadido. El disuasor trata de actuar sobre la mente de su enemigo, modificar su cálculo coste-beneficios para que le resulte negativo. El elemento físico es la fuerza disuasora, la capacidad bélica con la que amenazar al potencial agresor y con la que llevar a cabo la réplica o la resistencia si el ataque se produce. Esa fuerza debe ser de tal naturaleza y magnitud que haga la réplica (o resistencia) segura y eleve los costos de la aventura agresora por encima de los posibles beneficios. La probabilidad de la réplica y la cuantía probable de los daños son dos elementos esenciales del cálculo del agresor.

La especulación acerca de cuál es el castigo adecuado para disuadir y qué fuerzas son necesarias para ejecutarlo constituye una parte importante de los estudios acerca de la disuasión, precisamente aquella parte que tiene una mayor incidencia práctica en el diseño de una política de seguridad nacional. Pero lo que disuade es algo contingente. Depende de la evolución de la tecnología militar, de la naturaleza política del potencial agresor, de la correlación o balance de fuerzas y de la situación internacional. Depende, pues, de circunstancias cambiantes[8].

Ciberdefensa y ciberseguridad, conceptualizando

En un paso previo a visualizar algunos esbozos de enfrentamiento o mitigación a la amenaza, se hace necesario 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.

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 alcanzarlo. Entonces, la Defensa Nacional es el conjunto de medios materiales, humanos y morales que una nación puede oponer a las amenazas

8 Manuel Coma, *¿Qué es disuasión?*, Revista de Occidente número 78, noviembre 1987.

de un adversario en contra de sus intereses. 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.

Pero en el entendimiento del diseño y alcances de esa capacidad de ciberdefensa se generan confusiones que, más que ser conceptuales o semánticas, tienen impactos en la operacionalización de las acciones y recursos a emplear. Nace entonces la interrogante de la delimitación de la disyuntiva entre ciberdefensa y ciberseguridad.

Ciberdefensa

La ciberdefensa[9] es una connotación sistémica y sistemática que deben desarrollar los gobiernos y sus entes subordinados o asociados, 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.

Contempla la capacidad del Estado para prevenir y contrarrestar toda amenaza o incidente de naturaleza cibernética que afecte la soberanía nacional[10]. Por ello, la ciberdefensa[11] se relaciona con el desarrollo y aseguramiento de capacidades, preocupándose de sus recursos, actividades, tácticas y procedimientos para preservar la seguridad de los sistemas y la información que manejan, así como permitir la explotación y respuesta sobre los sistemas necesarios para garantizar el libre acceso al ciberespacio.

Como realidad complementaria de la ciberdefensa, se materializa el concepto de defensa nacional digital, en un conjunto de variables claves, en las que son necesarias el desarrollo de prácticas primordiales para darle sentido y real dimensión a la seguridad de una nación, en el contexto de

9 Jeimy Cano 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), pp. 4-7.

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

11 Jeimy Cano, *Ciberdefensa y Ciberseguridad, desafíos emergentes para los profesionales de Gobierno*, CFE, ECOPETROL.

una realidad digital y de información instantánea. Por ello, la ciberdefensa contendrá un conjunto de acciones de defensa activas, pasivas, proactivas, preventivas y reactivas para asegurar el uso propio del ciberespacio y negarlo al adversario en oposición.

Correlaciona entonces "un dominio global y dinámico dentro del entorno de la información, compuesto por una infraestructura de redes, de tecnologías de información y telecomunicaciones interdependientes, que incluye Internet, los sistemas de información y los controladores y procesadores integrados, junto con sus usuarios y operadores". Es de notar que incluye a usuarios y operadores, en realidad redundante, pues los sistemas por definición ya incluyen a las personas y los procedimientos.

Por ello, la ciberdefensa va notoriamente ligada al desarrollo y aseguramiento de capacidades.

Enfocándose en la conceptualización de ciberdefensa para el ámbito de la Defensa Nacional, estas son puntualizadas como "el conjunto de acciones en contra de ataques al Estado en el ciberespacio que se orientan a la defensa y supervivencia de sistemas militares"[12], materializándose mediante ciberoperaciones que otorgan la capacidad para operar militarmente en el ciberespacio donde la presencia en lo específico de ciberamenazas pueden afectar los sistemas C4I, redes de datos, nodos de comunicación, centros de procesamiento y lugares de almacenamiento de información, por lo que cumplen con los propósitos de seguridad (protección), inteligencia (recolección de información de la amenaza) y de respuesta (operaciones).

Por este motivo, las ciberoperaciones pueden ser ofensivas o defensivas, donde las primeras son acciones de respuesta sobre sistemas de información y comunicaciones adversarias, y las segundas corresponden a medidas preventivas, reactivas y de gestión de riesgo para dar protección a los sistemas, servicios y datos propios. De esta forma, el objetivo de estas operaciones será aportar a la solución del problema con una intencionalidad y un efecto deseado.

Ciberseguridad

Por su parte la ciberseguridad[13] puede ser entendida como el conjunto de actividades dirigidas a proteger el ciberspacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan. Entonces, asegura el uso de las redes propia y niega su empleo a terceros.

12 Santiago Aguayo, *Operaciones de Ciberdefensa*, Tesis ACAGUE, 2017.
13 Op. cit. Jeimy Cano.

A mayor abundamiento, el concepto de ciberseguridad es descrito[14] como "El conjunto de herramientas, políticas, conceptos de seguridad, directrices, métodos de gestión, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de una organización y a los usuarios en el ciberentorno". Por ello, comporta un conjunto de acciones de carácter preventivo que tienen por objeto asegurar el uso de las redes propias y negarlo a terceros[15].

La UIT (Unión Internacional de Telecomunicaciones) dice que la ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos, cuales son amenazas de seguridad correspondientes en el ciberentorno. Luego, 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.

Figura 1
Elementos de una estrategia de ciberseguridad

Fuente: Elaboración propia.

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

15 http://www.cari.org.ar/pdf/ciberdefensa_riesgos_amenazas.pdf

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).

Sintéticamente entonces, 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[16].

Por ello, la ciberseguridad va notoriamente ligada al desarrollo y aseguramiento de prácticas.

Debido a lo indicado, podemos concluir que la ciberseguridad tiende a ser un objetivo y la ciberdefensa apunta a ser un medio para su concreción.

En una analogía de los conceptos de Seguridad Nacional y Defensa Nacional, que sabemos se encuentran férreamente relacionados; también la ciberseguridad y la ciberdefensa en términos generales están estrechamente vinculados, la diferencia consiste en que la segunda tiene como propósito preservar la ciberseguridad, haciendo frente a un conjunto particular de riesgos y amenazas, los que identificados, controlados, neutralizados o contenidos darán paso a una condición de ciberseguridad.

Por ello, esa separación de aguas no es tan simple de delimitar, porque en la acción de la ciberdefensa de dar cabida a la condición de ciberseguridad, existirán espacios de interpenetración o traslapo, con áreas comunes donde ambos elementos se interrelacionan.

Acá es bueno traer a referencia a Feliú, quien acota que la ciberseguridad resulta ser un componente o aspecto muy importante de la Seguridad Nacional: Si no se controla adecuadamente el ciberespacio, desde allí una nación puede ver amenazada su libertad de acción y su Seguridad, no solo su ciberseguridad sino toda la Seguridad Nacional. El ciberespacio es pues un espacio estratégico a considerar al establecer la Estrategia de Seguridad y, como consecuencia, al planear la correspondiente Defensa Nacional, por lo que habrá que definir en ella los objetivos a alcanzar y las medidas de prevención, disuasión, protección y reacción de la ciberdefensa.

También la ciberseguridad y la ciberdefensa tienen puntos de encuentro en la forma cómo impulsan, aglutinan y coordinan los diferentes estamentos del Estado (incluidas sus Fuerzas Armadas y Policía), privados y académicos para generar un uso con libertad de acción del ciberespacio. Independiente de quién lidere estos esfuerzos, lo importante es que exista el concepto de empleo interagencial o multiactores, porque los esfuerzos de compartimientos

16 Op. cit. Consejo Nacional de Política Económica y Social de Colombia.

estancos poco o nada podrán hacer contra una amenaza que se presentará asimétrica, artera y sorpresiva.

Por ello se insiste que la ciberdefensa camina de la mano del desarrollo de las capacidades y la ciberseguridad del aseguramiento de las prácticas.

Infraestructuras de información de Defensa

Es entendida como un sistema interconectado de computadores/ordenadores, comunicaciones, aplicaciones de *data*, seguridad, personal, entrenamiento y otras estructuras que sirven a un sistema de defensa.

Luego, este proceso de manipulación por parte de un agresor y sus capacidades para tomar decisiones mediante el empleo de la ciberguerra, como uno de sus elementos, podrá actuar en busca de los siguientes objetivos[17]:

Seguridad informática: afectando la protección a la información y los sistemas informáticos, sus previsiones para el respaldo, restauración, detección y capacidad de reacción.
Entorno informático: saturando, perturbando, degradando o interrumpiendo la interacción de individuos, organizaciones o sistemas de búsqueda, proceso o difusión de información.
Superioridad informática: por medio de la negación de la capacidad del adversario de obtener, procesar y difundir información mediante un flujo ininterrumpido.
Sistema Informático: incidiendo en la eficacia de su infraestructura, organización, personal y componentes para degradar o neutralizar su capacidad de obtención, proceso, archivo, transmisión, proyección, difusión y acción.

La seguridad de las infraestructuras críticas

Las infraestructuras críticas, por definición, son sistemas físicos y basados en sistemas computacionales complejos que forman parte importante en una sociedad moderna y su funcionamiento fiable y seguro es de suma importancia para la vida económica y la Seguridad Nacional[18]. Si llegase a ocurrir un

17 DOD Directive S-3600.1, *Information Operations (IO),* Departamento de Defensa de Estados Unidos.

18 TEN, Chee-Wooi and LIU, Chen-Ching. *Cybersecurity for Critical Infrastructures: Attack and Defense Modeling*. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. July 2010. Vol. 40, no. 4, pp. 853-865. DOI 10.1109/TSMCA.2010.2048028.

incidente de seguridad en estos sistemas podría tener incluso conmoción a nivel nacional[19], consecuencias en los sistemas físicos que dependen de tales sistemas y mucha conmoción en la vida de los ciudadanos.

La seguridad física de la infraestructura de las plantas estratégicas es muy importante para evitar actos vandálicos comunes en subestaciones o plantas de gas. Sin embargo, la seguridad en redes es tan importante como la seguridad física, debido al impacto potencial que se puede alcanzar al manipular maliciosamente, por ejemplo, los sistemas remotos (SCADA o PLC-Programmable Logic Controller) de una planta eléctrica, de agua, gas, petróleo, cobre u otro tipo.

En seguridad informática, una vulnerabilidad implica que existen puntos débiles en la infraestructura tecnológica, políticas o de procedimientos, por lo que un atacante puede utilizar un conjunto de aplicaciones o métodos para romper la seguridad y explotar los puntos débiles en las redes y comprometer los sistemas. Por ello, la seguridad como tal está conformada por la confluencia de tres características[20], una tríada, que la configuran como tal, siendo estas: confidencialidad (*confidentiality*), integridad (*integrity*) y disponibilidad (*availability*).

La confidencialidad se refiere a mantener la *data* fuera de manos no autorizadas para su uso, empleo o conocimiento.

La integridad se orienta a la modificación no autorizada de *data* o funciones del sistema.

La disponibilidad corresponde a la capacidad de acceder a determinada *data* cuando ello es necesario.

Una de las actividades extendidas en ambientes de redes IT, para poder aplicar contramedidas a estas vulnerabilidades, consiste en adelantarse a las acciones maliciosas y realizar una intensiva búsqueda de brechas antes que un atacante real las descubra primero.

Un análisis de vulnerabilidades o *Ethical Hacking* es un buen comienzo para descubrir problemas de seguridad en redes y sistemas SCADA y pueden ser aplicados sin mayor inversión. Este tipo de actividad se puede transformar en el primer paso de un programa de seguridad informático con un enfoque holístico y de proceso para la administración de la infraestructura crítica.

En cuanto a infraestructuras críticas, y su definición de infraestructura de la información, es conformada por las personas, procesos, procedimientos,

[19] Juan Anabalón y Eric Donders, *Una Revisión de Ciberdefensa de Infraestructura Crítica*, Trabajo de titulación para obtener el grado de Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos de la Universidad de Santiago de Chile.

[20] J. Andress (2011). Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners, Estados Unidos, Syngress.

Figura 2
Triada de la seguridad

Fuente: Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners.

herramientas, instalaciones y tecnologías que soportan la creación, uso, transporte, almacenamiento y destrucción de la información. Dentro de las infraestructuras de la información, existe un conjunto especialmente relevante para la marcha del país, las denominadas infraestructuras críticas de la información (ICI), que comprende las instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya afectación, degradación, denegación, interrupción o destrucción pueden tener una repercusión importante en la seguridad, la salud, el bienestar de los ciudadanos y el efectivo funcionamiento del Estado y del sector privado. Las ICI se deberán robustecer, resguardar y diseñar para que sean seguras y resilientes frente a eventos que las puedan inhabilitar, adaptándose a cambios en el medio ambiente, a intervenciones humanas o interferencias informáticas, como incidentes involuntarios o ciberataques.

En cuanto a la identificación y jerarquización de las infraestructuras críticas de la información, aporta que los sectores que componen la clasificación de ICI son muy similares y se repiten en varias clasificaciones a nivel internacional. Luego, en una visión particular, esta determina que la infraestructura de la información de los siguientes sectores sea considerada como crítica: energía, telecomunicaciones, agua, salud, servicios financieros, seguridad pública, transporte, administración pública, protección civil y defensa, entre otras. Entonces, en algunos Estados ya existe una definición oficial para lo que es contenido bajo la categorización de infraestructura crítica de información,

determinada por las 10 áreas que enuncia, aun cuando queda abierta a "otras".

Al hablar de infraestructura crítica, como vemos, surge repetitivamente el concepto SCADA, que corresponde a *Supervisory Control and Data Acquisition*. Obedece a un concepto que mediante un *software* para ordenadores permite controlar y supervisar procesos industriales remotamente. Su diseño tiene la ventaja de entregar retroalimentación en tiempo real con los dispositivos desplegados en la instalación o terreno (sensores y actuadores), y controla el proceso automáticamente. Provee de toda la información que se genera en el proceso productivo (supervisión, control de calidad, control de producción, almacenamiento de datos, etc.) y permite su gestión e intervención.

Entre los procedimientos de acción remota están HMI (interfaz hombre-máquina) y SCADA, los que están relacionados entre sí en la medida en que uno o varios HMI son subconjuntos o componentes de un sistema SCADA[21]. Además, un DCS o Sistema de Control Distribuido es muy similar a un sistema SCADA, y también puede utilizar uno o más HMI también. Todos estos componentes son clases de, o describen partes de, un ICS o Sistema de Control, que es la descripción general de la automatización. En los sistemas de control modernos hay una gran cantidad de tecnología y funcionalidad entre estas dos clases de ICS.

Un sistema SCADA involucra control directo o comunicarse con uno o más de los siguientes:

Redes de automatización industrial y máquinas
Telemetría y control remoto utilizando comunicaciones continuas o ráfaga
Sistemas de control de procesos y control de procesos estadísticos
Sistemas de adquisición de datos (DAQ)
Históricos y servidores de almacenamiento de datos
Sistemas de control industrial utilizando PLC y RTU
Sistemas del entorno empresarial, como sistemas ERP y MES
Entorno de computación de nube industrial
Sistemas de seguridad y procesos
Seguridad de máquina local
Seguridad y control de procesos
Conectividad empresarial o global que implica LDAP y otros.

Un sistema SCADA puede estar conectado continuamente a todos los componentes en el ICS, o puede estar intermitentemente conectado a

21 Schneider Electric, ¿Cuál es la diferencia entre SCADA y HMI?

algunos o todos, y se actualiza con una ráfaga de comunicación por medio de módems de radio o celular (tecnologías 2G, 3G o 4G, CDMA y GSM, otras) a los dispositivos y equipos de campo. Así el SCADA suele tener uno o más servidores que contienen una aplicación que se está comunicando con una ejecución en conjunto con componentes inteligentes, independientemente del sistema SCADA.

Un Sistema de Control Industrial como se describe pueden conectarse entre sí mediante (uno o más de los siguientes) conexiones en serie, redes propietarias y/o Ethernet, LAN, WAN y/o la nube y puede incluir componentes externos ampliamente dispersos y/o instalaciones; incluir procesos tales como sistemas MES y ERP, Control de procesos y datos de historiadores, JIT y otros fabricantes de conectividad aguas arriba/aguas abajo, etcétera.

Debido a que los HMI, SCADA y sistemas de control son usados en muchos tipos de infraestructura que es crítica, su ventana de conectividad pasa a ser un blanco susceptible de una ciberagresión. La intrusión buscará penetrar los puertos de proceso directo y control de máquinas, automatización, seguridad, almacenamiento y análisis de datos, servicios de explotación indirectos, como el control de entrada / salida, comunicaciones y video, y conectividad a una variedad de funciones dentro del sistema de producción o servicio.

La seguridad en los sistemas SCADA anteriormente se mantenía físicamente, es decir, solo las personas con permisos de acceso a las instalaciones podían obtener los datos, por tanto la seguridad computacional no era preocupante.

La convergencia de las redes de datos industriales con las redes de datos de TI ha proporcionado nuevas vías de acceso a estos sistemas, lo que implica a su vez que los riesgos de seguridad asociados históricamente a las redes IT ahora también son de preocupación de las redes operacionales (OT)[22].

El problema fundamental de los sistemas SCADA, ampliamente utilizados en infraestructuras críticas, es que nunca fueron pensados ni diseñados con sistemas de seguridad informática, ni tampoco se han elaborado con la mentalidad de seguridad desde el proceso mismo de desarrollo de *software*, algo que incluso aún no se considera completamente en el proceso de diseño de programas para sistemas que no son de la naturaleza de los sistemas de control industrial[23]. Muchos sistemas SCADA utilizan sistemas de autenticación muy básicos, sin protocolos de cifrado de datos e infraestructura con muchos *bugs* de seguridad y totalmente desactualizada, este escenario se agrava por

[22] Op. cit. Juan Anabalón y Eric Donders.

[23] Daniel Mellado, Eduardo Fernández-Medina, and Mario Piattini,. Security requirements engineering framework for software product lines. Information and Software Technology. October 2010. Vol. 52, no. 10, p. 1094-1117. DOI 10.1016/j.infsof.2010.05.007.

el hecho de que la actualización de una plataforma muchas veces implica la actualización de sistemas relacionados, lo que para la industria energética y otra infraestructura crítica es casi imposible desarrollar sin detener los servicios que provee[24].

En Chile se han desarrollado algunos estudios de infraestructura crítica a nivel gubernamental por distintas secretarías de Estado. En el caso de la infraestructura crítica de telecomunicaciones se refiere a "aquellas redes cuya interrupción o destrucción podría producir un serio impacto en la salud, seguridad o bienestar de la población o producir un serio impacto en el funcionamiento del gobierno o de la economía del país"[25].

En este sector, los elementos de red más críticos corresponden a las redes de transporte de la señal de comunicaciones, ya que están seriamente expuestos a amenazas de tipo físico debido a que sus componentes están emplazados en espacios no controlados. Estas redes cuentan con respaldos de otros operadores, sin embargo la cercanía que existe entre sí, en ciertos tramos, reducen la efectividad esperada. Además, existen sitios (edificios) de los distintos operadores altamente concentrados en cuanto a redes y nodos, que los transforman en importantes puntos de falla en caso de amenazas. Sin embargo, los operadores de telecomunicaciones trabajan cooperativamente y se respaldan mutuamente y cada operador cuenta con los sistemas de protección en sus redes y nodos que permiten proveer servicios con alto nivel de disponibilidad.

En este actuar, estudio, diseño, planificación, conducción y evaluación concurren no solo militares sino que también civiles, participando como unidades u organizaciones estructuradas (no necesariamente reconocidas), pasando por células aisladas pero orientadas desde un nivel coordinador superior, hasta el ciberguerrero aislado (*broken arrow*).

Amenazas en el ciberespacio

La amenaza es definida[26] como "la percepción de la capacidad que un potencial adversario posee para infligir un daño o perjuicio, especialmente si

[24] Op. cit. Juan Anabalón y Eric Donders.

[25] Zagreb, Consultores Ltda., Subsecretaría de Telecomunicaciones y Ministerio de Transporte y Telecomunicaciones. Estudio para la definición e identificación de infraestructura crítica de la información en Chile. Diciembre 2008.

[26] Op. cit. Santiago Aguayo, Operaciones de Ciberdefensa.

no se actúa como él desea"[27]. Complementa esto Timothy K. Buennemeyer[28] al aportar una definición que logra relacionar ciberespacio y amenaza, estableciendo que "El ciberespacio se ha transformado rápidamente en un ambiente volátil, incierto, complejo y ambiguo, donde los gobiernos, empresarios e individuos requieren un balance de información que contemple la trilogía de confidencialidad, disponibilidad e integridad, en orden a establecer un modelo de seguridad de la información estable". Agrega que "la confidencialidad es el término usado para describir la prevención de difusión de información a individuos o sistemas no autorizados". Continúa aportando que en seguridad de la información, integridad implica que la *data* no puede ser modificada sin que ello sea detectado. Del análisis de esta expresión se deduce que existe una caracterización del ciberespacio y su entorno, como también las actividades que se deben realizar para impedir su afectación por parte de las amenazas, que considerará ciertas acciones destinadas a impedir la divulgación de información virtual a las personas o sistemas no autorizados, pese a que no se entrega una definición de cuáles son.

Así pues, el desarrollo del ciberespacio ha facilitado enormemente el impulso de toda clase de actividades, incluyendo interacciones comerciales, sociales y gubernamentales[29], constituyendo una dimensión importante para los Estados, organizaciones y las personas y, por consiguiente, la seguridad del ciberespacio ha crecido en importancia frente a las amenazas. "Debido a que la sociedad actual depende ampliamente de las tecnologías de la información (TI), esto conlleva la irrupción de nuevas amenazas desconocidas en el pasado. En virtud del carácter global de las redes, los incidentes de seguridad de las TI que les afecten, pueden ocasionar interrupciones o fallos permanentes en la infraestructura de información del país"[30]. Esto deja en evidencia la vinculación de la información que circula por medio de las redes respecto de potenciales amenazas en este escenario virtual, que asociándolos al entorno en que se originan entran en la definición de "ciberamenazas".

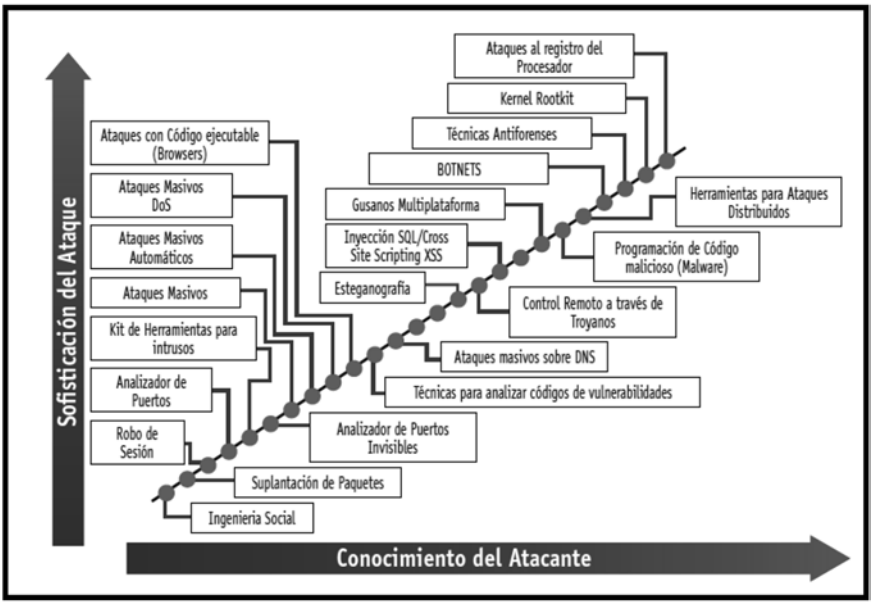
27 Luis Feliú Ortega. "La Ciberseguridad y La Ciberdefensa". En Monografías del CESEDEN Nº 126. El Ciberespacio. Nuevo Escenario de Confrontación, de Centro Superior de Estudios de la Defensa Nacional. Madrid: Imprenta del Ministerio de Defensa, 2012, p. 40.

28 Timothy K. Buennemeyer, "A Strategic Approach to Network Defense: Framing the Cloud". Parameters 45, no. 3 (Autumn, 2011) ProQuest Military Collection p. 45.

29 José L. González Cussac, "Estrategias legales frente a las Ciberamenazas", en *Cuaderno de Estrategia* Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, de Instituto Español de Estudios Estratégicos, Madrid: Imprenta del Ministerio de Defensa, 2010, pp. 259-322.

30 P. Acosta, "Seguridad nacional y ciberdefensa" (2009). http://catedraisdefe.etsit.upm.es/wp-content/uploads/2010/07/CUADERNO-N%C2%BA-6.pdf.

Figura 3
Conocimiento del atacante vs. sofisticación del ataque



Fuente: "Ciberdefensa y ciberseguridad: dos elementos de la Ciberguerra" (Memorial del Ejército de Chile, agosto, 2014).

En este contexto y considerando la tipología de las amenazas que pueden afectar a los sistemas[31], estas pueden ser agrupadas en:

- Desastres naturales.
- Amenazas de origen industrial.
- Errores o fallos no intencionados.
- Ataques deliberados.

No obstante las amenazas asociadas a desastres naturales, las de origen natural y las relacionadas con errores o fallos no intencionados siempre estarán presentes, es necesario profundizar en los ataques deliberados, porque su sofisticación, precisión y posible impacto está en continua evolución y elevan el nivel de riesgo al que están sometidos los sistemas.

Dependiendo de la motivación de dichos ataques, estas amenazas pueden ser agrupadas en los siguientes tipos:

31 Op. cit. Ricardo Mesa Illés, archivo CEEAG, 2016.

- **Cibercrimen**: centradas en la obtención de beneficios económicos mediante la realización de acciones ilegales.
- **Ciberespionaje**: centradas en la obtención de información, sea para beneficio propio o para obtener un beneficio monetario posterior a su venta.
- **Ciberterrorismo**: donde se busca un impacto significativo mediante la destrucción física. Así las infraestructuras críticas pueden ser uno de los objetivos más probables de ser atacados.
- **Ciberguerra**: la lucha o el conflicto entre dos o más naciones o diferentes bandos dentro de una nación, donde el ciberespacio es el campo de batalla.
- **Hacktivismo**[32] **o ciberactivismo**: que también podría ser considerado como un campo de acción de la ciberamenaza (Escuela de Altos Estudios de la Defensa, 2014).

Asimismo, tomando en consideración las motivaciones de las fuentes de dichas amenazas y su probabilidad de ocurrencia, es que estas se pueden clasificar en:

- Cibercriminales.
- Espías industriales.
- Hacktivistas.
- Terroristas.
- Naciones.
- Hackers.
- Personal interno.

Por otra parte, las motivaciones, que pueden ser independientes del origen de la amenaza, podrían clasificarse en:

- **Beneficios económicos**: es la más usual en el ciberespacio y consiste en la realización de actos fraudulentos, robo y venta de información o la ejecución de ataques.
- **Ventaja táctica o competitiva**: una forma de llevarla a cabo es mediante el robo de información de una nación en medio de un conflicto y que

[32] El hacktivismo es la piratería motivada políticamente llevada a cabo por grupos como Anonymous o LulzSec. Se trata de ataques que tienen como objetivos interrumpir la actividad normal de las instituciones públicas y aquellos organismos contrarios a los valores defendidos por estas agrupaciones de personas. http://www.pcworld.com.mx/Articulos/23891.htm.

puede dar una ventaja táctica al enemigo. Las naciones y los espías son los agentes con más probabilidad de tener esta motivación.
- **Motivaciones políticas**: diferentes organizaciones podrían atacar o realizar acciones perjudiciales contra los gobiernos u organizaciones públicas.
- **Destrucción o daño**: esta motivación puede ser asociada a terroristas, ya que pueden buscar la ejecución de ataques que tengan este efecto. Las naciones en conflicto también podrían estar dentro de este grupo.
- **Fama o venganza**: principalmente ligada a los *hackers*[33] que buscan reconocimiento dentro de sus comunidades. Su objetivo no es causar daño, aunque podrían acceder a información sensible.

La Organización del Tratado del Atlántico Norte (OTAN) a partir del 2010, consciente del riesgo de las ciberamenazas, creó un plan estratégico que consideraba que los ciberataques estaban entre las tres amenazas más probables a la Alianza. Lo anterior se basa en la tendencia general que establece que a mayor desarrollo de un país existirán una mayor cantidad de elementos vulnerables que afecten a su seguridad, aumentando proporcionalmente la exposición frente a estas amenazas, concibiéndose algunas acciones para defenderlas, lo que es inclusivo para los sistemas C4I de cualquier nivel, ya que son altamente dependientes del ciberespacio, no tan solo en el ámbito militar, sino además como parte de las denominadas infraestructuras críticas de una Nación.

Concordemente, esta perspectiva ya se encuentra estipulado en las Tendencias estratégicas globales del Ministerio de Defensa de Gran Bretaña hacia el 2045 publicadas en el 2014, donde se aprecia una declaración al respecto y que orienta una visión estratégica en esta política sectorial, al establecerse que "existirá un incremento en la amenaza de ciberataques provenientes de criminales y terroristas, toda vez que la infraestructura crítica nacional se vuelve más integrada a las plataformas de información y comunicación[34]".

De modo que, de acuerdo con lo expresado por González Cussac[35], la concepción de ciberamenazas estará conformada por los ataques perpetrados

[33] Un *hacker* es aquella persona experta en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo. http://www.definicionabc.com/tecnologia/hacker-2.php. (último acceso: 18 de diciembre de 2015).

[34] United Kingdom's Ministry of Defence, "Strategic Trends Programme Global Strategic Trends-Out to 2045" (en línea) [fecha de consulta 20.08.2016] https://www.gov.uk/government/publications/global-strategic-trends-out-to-2045.

[35] José L. González Cussac, "Estrategias legales frente a las Ciberamenazas", en *Cuaderno de Estrategia* Nº 149 Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio,

o patrocinados por Estados (ataques a infraestructuras críticas), ataques cometidos por grupos terroristas o por cualquier otra manifestación de extremismos, ya sean políticos, ideológicos o religiosos. Al respecto, surgen los ataques de la delincuencia organizada denominado "cibercrimen" y, por último, los ataques de bajo perfil, los que por su naturaleza muy heterogénea afectan transversalmente a las personas incluyendo desde intromisiones en la información personal hasta pequeños fraudes.

En síntesis, el ciberespacio es la expresión de un espacio virtual y vital para que exista la transmisión de la información, razón por lo que se desarrollarán sucesivas acciones de amplia variedad para ejercer el control y la protección de las redes informáticas, originando por consecuencia la necesidad de asegurar el funcionamiento de estos sistemas frente a diversas amenazas, definidas como ciberamenazas; cuyos efectos son traslapados desde lo virtual a lo físico generando en los Estados y sus habitantes múltiples e insospechadas consecuencias que afectan los derechos de las personas, las infraestructuras críticas de la información y, por esta razón, los intereses vitales de Chile a nivel nacional e internacional.

Respecto de la clasificación y estratificación de amenazas, el CARI (Consejo Argentino para las Relaciones Internacionales) genera un muy completo trabajo académico que es traído como referencia. En su caracterización de las amenazas[36] da cuenta de una estructuración de acuerdo con diferentes elementos distintivos, como sigue:

Amenazas por el origen

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de que la red no esté conectada a un entorno externo, como Internet, no nos garantiza la seguridad de la misma. De acuerdo con el Computer Security Institute (CSI) de San Francisco, aproximadamente entre el 60 y 80 por ciento de los incidentes de red son causados desde dentro de la misma. Basado en el origen del ataque podemos decir que existen dos tipos de amenazas:

de Instituto Español de Estudios Estratégicos. Madrid: Imprenta del Ministerio de Defensa, 2010, p. 93.

36 Ciberdefensa-Ciberseguridad Riesgos y Amenazas CARI. Noviembre 2013.

Amenazas externas y amenazas internas

***Amenazas internas**:* generalmente estas amenazas pueden ser más serias que las externas. Los usuarios o personal técnico conocen la red y saben cómo es su funcionamiento, ubicación de la información, datos de interés, etc. Además tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo, lo que les permite unos mínimos movimientos. Los sistemas de prevención de intrusos o IPS, y *firewalls* son mecanismos no efectivos en amenazas internas, porque habitualmente no están orientados al tráfico interno.

***Amenazas externas**:* se originan fuera de la red local. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos. Para clasificarlo como externo debe ser exclusivamente por personas ajenas a la red, podría ser por vulnerabilidades que permiten acceder a la red: rosetas, *switches* o *Hubs* accesibles, redes inalámbricas desprotegidas, equipos sin vigilancia, etcétera.

Amenazas por el efecto: el tipo de amenazas por el efecto que causan a quien recibe los ataques podría clasificarse en robo de información, destrucción de información, anulación del funcionamiento de los sistemas o efectos que tiendan a ello, suplantación de la identidad, publicidad de datos personales o confidenciales, cambio de información, venta de datos personales, etc. robo de dinero, estafas, otras.

Amenazas por el medio utilizado: se pueden clasificar por el *modus operandi* del atacante, si bien el efecto puede ser distinto para un mismo tipo de ataque. En esta clasificación tienen cabida los virus informático o *malware*, que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus habitualmente reemplazan archivos ejecutables por otros infectados con el código de este, así pueden destruir, de manera intencionada, los datos almacenados en una computadora, aunque también existen otros más inofensivos, que solo se caracterizan por ser molestos (*Worms*, *BOTs*, *Adware*, *Cookies*, *Phishing*, etc.).

Los atacantes pueden tener a su favor el tiempo de preparación, prácticamente sin límite. Sus campañas, que con frecuencia aprovechan las vulnerabilidades conocidas que las organizaciones y los usuarios finales pueden tener –y deberían conocer y abordar– permanecen activas e inadvertidas durante días, meses o incluso más tiempo. Los defensores, mientras tanto se esfuerzan para obtener visibilidad de la actividad en torno a las amenazas y por reducir el tiempo de detección (TTD) de las amenazas nuevas y conocidas[37].

[37] http://www.cisco.com/c/dam/m/es_mx/offers/assets/pdfs/cisco_2016_mcr_es-xl.pdf

Las principales ciberamenazas[38]

Ataque DDoS	Saturar un servidor haciendo más conexiones de las que puede soportar. En 2014, una compañía energética española fue víctima de un ataque mediante ordenadores zombis, infectados por un troyano. Duró tres horas y se recibieron 119 millones de conexiones que tumbaron el servicio.
Troyanos	Como el caballo de Troya, entran subrepticiamente en un sistema. Aprovechan una puerta trasera para ejecutar programas sin permiso.
Gusanos	Virus capaces de duplicarse por sí mismos y de hacer que las máquinas que los hospedan sean cada vez más lentas.
Keyloggers, stealers	Programas para robar datos.
Botnets	Redes de ordenadores infectados o zombis. Pueden, por ejemplo, hacer millones de clics en un *banner* haciendo creer al cliente que su promoción está teniendo éxito, cuando no es así.
Amenaza avanzada persistente	Conjunto de procesos informáticos sigilosos y continuos, dirigidos sobre todo a romper la seguridad informática de una empresa para realizar espionaje industrial o encontrar vulnerabilidades de seguridad.
Backdoor	Puerta trasera, entrada en un PC sin ser detectado, generalmente para someterlo a un acceso remoto.
Drive by downloads	Sitios que instalan códigos (*spyware*) que dan información de los equipos sin que se percate el usuario.
Ransomware	Programas que hacen inaccesibles archivos. Cifran, por ejemplo, el disco duro. El ciberagresor pide un rescate para que el afectado pueda recuperar la información.
Ataque de día cero	Es un ataque contra una aplicación o sistema que ejecuta código malicioso gracias al conocimiento de vulnerabilidades que son desconocidas para la gente y el fabricante del producto. Esto supone que aún no se conocen antivirus o herramientas para repararlas.

[38] http://www.xlsemanal.com/conocer/20150719/cuartel-general-antihackers-8672.html

Reflexiones finales

El ciberespacio ha pasado a constituir un factor estratégico que requiere la imperiosa atención permanente del ámbito de la defensa, orientando a ser incorporada y mantenida dentro de la estrategia de seguridad de todo Estado, llamando así a definir en ella objetivos por alcanzar medidas de prevención, disuasión, protección y reacción de la ciberdefensa, que generen un centinela estructural que vele por amenazas dinámicas que se caracterizan por su sofisticación, precisión y grado de impacto, lo que está en continua evolución y elevan el nivel de riesgo al que están sometidos los sistemas.

La ciberdisuasión impone una visión moderna de aplicación, porque es inviable hacer una demostración de capacidades de ciberguerra con una finalidad exclusivamente intimidatoria, desafiante o de potencial coacción. Así, la lógica de la ciberguerra entrega ventajas comparativas al contendiente que decide tomar la iniciativa y lanzar el primer ataque, porque técnica y estratégicamente la existencia de un sistema de alerta temprana y anticipación es muy difícil, como también el concepto de "profundidad estratégica", en su vertiente clásica, está ausente. Esto crea un entorno estratégico marcado por la incertidumbre, tremendamente inestable, donde el éxito de la disuasión se potenciará por nuestra capacidad de convencer a los adversarios que sus intrusiones cibernéticas implicarán un costo demasiado alto para ellos, evento ante el cual aún podremos seguir operando por contar con un grado de resiliencia, pese a que esta sea local, parcial, temporal e imperfecta.

De no haber optado por la iniciativa, en su analogía de dar el primer cibergolpe, uno de los cursos de acción a considerar es la respuesta en masa, concatenada en el máximo de medios simultáneos, sobre efectos vinculados y orientados principalmente a infraestructura crítica, solución que debemos tener en vista tanto para un enfoque ofensivo como defensivo del problema estratégico.

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.

Aguayo Santiago. *Operaciones de Ciberdefensa*, Tesis ACAGUE, 2017.

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

Anabalón, Juan y Donders, Eric. *Una Revisión de Ciberdefensa de Infraestructura Crítica*, Trabajo de titulación para obtener el grado de Magíster en Seguridad, Peritaje y Auditoría en Procesos Informáticos de la Universidad de Santiago de Chile.

Andress J. Cyber Warfare, Techniques, Tactics and Tools for Security Practitioners, 2011, Estados Unidos, Syngress.

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.

Buennemeyer, Timothy K. "A Strategic Approach to Network Defense: Framing the Cloud." Parameters 45, no. 3, 2011.

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.

CARI, Ciberdefensa-Ciberseguridad Riesgos y Amenazas, Noviembre 2013.

Coma, Manuel. *¿Qué es disuasión?*, Revista de Occidente número 78, Noviembre 1987.

Cubeiro, Enrique. *Conciencia nacional de ciberdefensa*, Centro Superior Estudios de la Defensa Nacional (CESEDEN), Jornadas Construyendo la Ciberdefensa en España.

Chee-Wooi, TEN and Chen-Ching, LIU. *Cybersecurity for Critical Infrastructures: Attack and Defense Modeling*. IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans. July 2010.

Dershowitz, Alan. *Por qué aumenta el Terrorismo*, Ediciones Encuentro, Madrid.

DOD Directive S-3600.1. *Information Operations (IO),* Departamento de Defensa de Estados Unidos.

Feliú Ortega, Luis. *La Ciberseguridad y La Ciberdefensa.* En Monografías del CESEDEN Nº 126. El Ciberespacio. Nuevo Escenario de Confrontación, de Centro Superior de Estudios de la Defensa Nacional. Madrid: Imprenta del Ministerio de Defensa, 2012.

González Cussac, José L. "Estrategias legales frente a las Ciberamenazas", en *Cuaderno de Estrategia* Nº 149. Ciberseguridad. Retos y Amenazas a la Seguridad Nacional en el Ciberespacio, de Instituto Español de Estudios Estratégicos. Madrid: Imprenta del Ministerio de Defensa, 2010.

Howard, M. Reasurance and Deterrence, *Western Defense in the 1980's*, Foreign Affaires, 61 (winter 1982-1983).

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.

Mellado, Daniel; Fernández-Medina, Eduardo; Piattini, Mario. Security requirements engineering framework for software product lines. Information and Software Technology. October 2010.

Mesa Illés, Ricardo. *La Ciberguerra: una proposición, Academia de Guerra, Ejército de Chile, archivo CEEAG,* 2016.

Observatorio, CEEAG, septiembre, 2016.

Pintado Rodríguez, César. *De la Guerra (Asimétrica)*, Boletín 55/2014, 19 mayo de 2014, Instituto Español de Estudios Estratégicos

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

Rhea, Siers. *Mitos de la Ciber Disuasión*, The Cipherbrief.

Riveros, Edgardo. Subsecretario de Relaciones Exteriores, Seminario Internacional "Ciberseguridad y Ciberdefensa en Chile", 27 de noviembre de 2015, Aula Magna, Facultad de Derecho, Universidad de Chile.

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.

Schneider Electric. ¿Cuál es la diferencia entre SCADA y HMI?

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.

Zagreb, Consultores Ltda. Subsecretaría de Telecomunicaciones y Ministerio de Transporte y Telecomunicaciones. Estudio para la definición e identificación de infraestructura crítica de la información en Chile. Diciembre 2008.

Capítulo 4

El desafío del combate por el mando y control

*Mario Arteaga Velásquez**

Introducción

El concepto de "ciberguerra" sigue siendo tema de discusión, a tal punto que se ha convertido en un inevitable tópico de debate en el ámbito de la seguridad internacional debido a que se le atribuye ambigüedad y se le califica de controversial. Por otra parte, también persiste la tendencia a confundir ciberguerra con ciberataques, siendo pertinente revisar el aporte de Javier Jordán y Josep Baqués al respecto, porque ambos se encargan de transmitir la conceptualización de ciberguerra que propone Adam P. Liff al manifestar que ella constituye "una situación de conflicto entre dos o más actores políticos, caracterizada por la ejecución de ataques deliberados, hostiles y dañinos contra redes de ordenadores en la infraestructura crítica civil o militar de un adversario con intención coercitiva y orientada a la obtención de concesiones políticas; o como una medida de fuerza bruta contra redes militares o civiles con el fin de reducir la capacidad del adversario para defenderse o para llevar a cabo represalias semejantes o mediante fuerzas convencionales, así como contra objetivos militares o civiles con objeto de afectar a un actor

* Mario Arteaga Velásquez es General de División (R) del Ejército de Chile. Doctor en Relaciones Internacionales, Universidad Complutense de Madrid. Magíster en Ciencias Militares con mención en Política de Defensa, Academia de Guerra del Ejército de Chile. Magíster en Ciencias Militares con mención en Planificación y Gestión Estratégica, Academia de Guerra del Ejército de Chile. Diplomado en Gestión Educacional, Pontificia Universidad Católica de Chile. Director ejecutivo del Centro de Estudios Estratégicos de la Academia de Guerra del Ejército de Chile. marteagav@acague.cl

por motivos estratégicos"[1]. De lo expresado por Liff se infiere que los ciberataques constituyen acciones que son parte de la ciberguerra, que esta última compromete a actores políticos como son los Estados; y que el propósito es obtener ventajas políticas y estratégicas que impidan la respuesta del adversario.

Según Manuel R. Torres, existen analistas quienes sostienen que la tierra, el mar, el aire, el espacio y el ciberespacio son los cinco "dominios" donde se puede "librar la guerra"[2]. Luego, es lógico considerar que tanto las acciones ofensivas como las defensivas, en las que se lleva a efecto la ciberguerra, tienen como escenario lo que los Estados reconocen como el "quinto dominio", es decir, el ciberespacio, que además es considerado "como una zona de combate" donde es posible realizar actividades que cada día tienen un mayor impacto en las capacidades civiles y militares de los mismos Estados, atendiendo a que los objetivos corresponden, entre otros, a las funciones económicas, las funciones gubernamentales, la infraestructura vital del Estado, la estructura militar y, particularmente, la estructura de mando y control política y estratégica.

El ciberespacio es un ámbito o dominio extremadamente complejo, porque allí se facilita la ejecución de las acciones defensivas y se dificulta la ejecución de las acciones ofensivas; también, porque los límites son indefinidos y ello dificulta la detección y la identificación del adversario y, menos aún, se pueden determinar con algún grado de certeza la magnitud y capacidad de este mismo. Se suma a lo anterior, que el ciberespacio no constituye el escenario absoluto de la ciberguerra porque, así como lo sostiene Liff, las acciones que ella considera pueden ser llevadas a efecto por fuerzas convencionales, lo que significa accionar en los otros dominios (tierra, mar, aire y el espacio) para reducir la capacidad de respuesta del adversario.

En el debate respecto de los dominios existen autores que sostienen la existencia de dominios físicos y abstractos, situando al ciberespacio entre los últimos. Además, identifican al espectro electromagnético como un dominio independiente, junto con el ambiente de la información y el dominio cognitivo, considerando que todos ellos se localizan entre los abstractos. Al respecto, se estima que el espectro electromagnético sería parte del dominio del ciberespacio, en tanto se considera y acepta que la guerra electrónica se desarrolla en dicho espectro y que ella corresponde a uno de los elementos del combate por el mando y el control que tiene ocurrencia en el ciberespacio. Respecto del ambiente de la información y al dominio cognitivo, se estima

1 Javier Jordán y Josep Baqués. *Guerra de Drones: Política, tecnología y cambio social en los nuevos conflictos,* Madrid: Editorial Biblioteca Nueva, S.L., 2014, p. 130.

2 Manuel R. Torres. *Ciberguerra,* en: Javier Jordan: Manual de Estudios Estratégicos y Seguridad Internacional, Madrid: Plaza y Valdés S. L., 2013, pp. 331-333.

que ambos son parte de la guerra por la información y del combate por el mando y control, razón por la que no constituirían dominios sino que bastaría con identificarlos como condiciones que influyen en la toma de decisiones que se producen en los cinco dominios identificados con anterioridad. Como sea, lo anterior es algo que se tendrá que continuar analizando en el futuro.

Se ha establecido que existe una relación entre ciberguerra, guerra de información, mando y control y ciberespacio, pero junto con mantener el esfuerzo para conocer aún más de ellos, se advierte que es necesario investigar y reflexionar respecto del combate por el mando y control, de tal manera que sea posible identificar los factores que intervienen, las amenazas que puedan afectarle y las condiciones y desafíos para alcanzar la victoria en el citado combate. Esta tarea, de por sí compleja, se dificulta más considerando que la ciberguerra y su objeto de estudio, el combate por el mando y control, ocurren preferentemente en el ciberespacio que, como ya se dijo, es un dominio de extrema complejidad. Para dar respuesta a las inquietudes expresadas anteriormente, en este artículo se intenta establecer cómo alcanzar la victoria en el combate por el mando y control. Para ello, en la primera parte se aborda la relación entre la guerra de información y el mando y control en el ciberespacio. A continuación, en la segunda parte, se examinan los elementos que intervienen en el combate por el mando y control. Luego, en la tercera parte, se analizan las condiciones y desafíos para combatir por el mando y control con éxito. Finalmente se presentan algunas conclusiones que responden a la interrogante referida a cómo alcanzar la victoria en el combate por el mando y control.

El ciberespacio y el combate por el mando y control

El ciberespacio, según las Fuerzas Armadas de Estados Unidos, corresponde al "dominio global del ambiente de información que consta de infraestructuras de tecnología de información en redes interdependientes y datos residentes, incluyendo Internet, redes de telecomunicaciones, sistemas computarizados, además de procesadores y controladores integrados"[3].

Otros analistas, con los cuales se concuerda, complementan lo anterior señalando que en el ciberespacio se lleva a efecto una verdadera competencia, con características propias de la guerra, para ello se requieren capacidades

[3] Michael Kolton. *La seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización futuras*, en: Military Review, Centro de Armas Combinadas, Fort Leavenworth, Kansas, Mayo-Junio 2016, p. 52.

que permitan afrontar los esfuerzos que permitan conducir política y estratégicamente el empleo del poder del Estado.

Por otra parte, anteriormente se indicó que la ciberguerra se relacionaba con la lucha por la información y que constituía una situación de conflicto entre actores políticos, los Estados, que realizan acciones coercitivas entre ellos recurriendo a la utilización del Poder Nacional, donde destaca el empleo de la capacidad militar. Refuerza lo anterior el hecho de que el combate por el mando y control implica una situación de conflicto y la ejecución de acciones para imponerse al adversario con el propósito de conseguir el dominio; de esto se infiere que la lucha por la información y el combate por el mando y control se encuentran relacionados.

Ahondando en el concepto de mando y control, es importante tener presente que este se distingue por ser el encargado de proveer la información necesaria para que la toma de decisiones se produzca con el menor grado de incertidumbre y con la mayor rapidez y oportunidad posible, de tal manera que la acción propia se anticipe a la del adversario, considerando, además, que también contribuye a la convergencia de los esfuerzos nacionales tanto políticos, económicos, diplomáticos como militares en beneficio del logro de los propósitos establecidos mediante la aplicación de la unidad de mando. Un asunto importante en lo referido al mando y control es que en pleno siglo XXI aún se debate acerca de la forma de llevarlo a efecto; y es así como algunos adhieren a la práctica del mando y control detallado, que se caracteriza por la emisión de órdenes que restringen la libertad de acción de los escalones subordinados y por la aplicación de sistemas de control que tienden a invadir los espacios de acción inferiores, con lo que la libertad de acción se restringe aún más. Por el contrario, existen otros que privilegian la práctica del mando y control directivo, que se distingue por el otorgamiento de libertad de acción para que los escalones subordinados puedan actuar aplicando su iniciativa orientados por la intención del escalón superior.

Es indudable que el ambiente político, estratégico u operacional influirá cuando se tenga que decidir el tipo de mando y control a utilizar; sin embargo, antes de hacerlo es conveniente recordar que las restricciones de libertad de acción inhiben la iniciativa y con ello se retarda el accionar. Lo más grave es que lo anterior puede transformarse en una pérdida de la libertad de acción general y que ello podría afectar la toma de decisiones en los niveles superiores, generándose un ambiente donde impere la voluntad del adversario. El asunto adquiere mayor complejidad al considerar que la acción de mando y control se ejecuta preferentemente en el ciberespacio, porque es en ese ambiente donde acciona la infraestructura de información y se produce la interdependencia de las redes, como fue mencionado anteriormente.

Jim Dunivan[4], refiriéndose al mando y control, sostiene que Sun Tzu, Von Clausewitz, Jomini y Von Molke, entre otros, coinciden en que la rápida toma de decisiones es fundamental para mantener la iniciativa y que de no hacerlo se corre el riesgo de ceder esa iniciativa al adversario y por consiguiente la libertad de acción que pasa a manos de ese adversario. Poseer libertad de acción significa disponer de una capacidad esencial para actuar sin que se oponga la voluntad de un adversario, ella facilita el cumplimiento de la propia intención y para obtenerla es indispensable aplicar la iniciativa, la sorpresa y la seguridad. Es improbable alcanzar un grado de libertad de acción absoluto, porque así como ella es indispensable para el cumplimiento de la propia intención, también lo es para que un eventual adversario pueda cumplir la suya, por tanto será necesario realizar acciones para impedir que ese adversario llegue a poseerla; y si cuenta con ella, realizar las acciones necesarias para que la pierda[5]. Lo anterior corresponde a la histórica lucha por la libertad de acción, donde la forma de ganarla, mantenerla y asegurarla constituye un desafío para los conductores políticos y militares, porque, finalmente, estar en posesión de ella significa disponer de oportunidades políticas y militares que favorezcan la propia intención.

En los niveles más altos de la organización del Estado, la libertad de acción para la toma de decisiones adquiere una importancia equivalente a la de los intereses nacionales, porque constituye un elemento fundamental para resolver con autonomía durante los procesos interestatales; y es por ello que debe ser protegida al igual que ocurre con los intereses nacionales citados anteriormente[6]. En el ámbito militar, especialmente en lo estratégico y en lo operacional, la libertad de acción es una condición fundamental para la toma de decisiones alejada de la atrición que provenga del adversario, lo que implica que este último debe estar afectado por la pérdida de la iniciativa y, por consecuencia, sometido a una condición reactiva, es decir, respondiendo a la presión de su oponente. Cuando un actor se encuentra en las condiciones descritas, es decir, sin iniciativa y reaccionando permanentemente, es altamente

4 Jim Dunivan. *C2 en el campo de batalla digitalizado: ¿Cediendo la iniciativa?* Military Rewiew, Fort Leavenworth, Kansas, March-April 2004, pp. 2-4.

5 André Beaufre. *Introducción a la Estrategia,* Madrid: Instituto de Estudios Políticos, 1965, p. 157. Beaufre sostiene que "la lucha por la libertad de acción es, en efecto, la esencia de la estrategia" y que su protección se obtiene mediante la seguridad, en tanto que la privación de ella para el adversario es el producto de la propia iniciativa combinada con la sorpresa. Señala, además, que ambos dan origen a un "juego estratégico".

6 Alexander Wendt. *Social Theory of International Politics,* United Kingdom, Cambridge: Cambridge University Press, 2006, p. 235. Según Wendt, Alexander George y Robert Keohane identifican tres intereses nacionales: supervivencia física, autonomía y desarrollo económico. Es por ello que la libertad de acción, si bien no constituye un interés nacional propiamente tal, contribuye a la obtención de uno de ellos: la autonomía.

probable de que se produzca la parálisis política, estratégica u operacional, que no es otra cosa que estar imposibilitado para continuar conduciendo el empleo de sus capacidades de manera coordinada y orientada al punto donde deben concentrase los esfuerzos para conseguir el éxito[7]. Cuando se consigue la parálisis del adversario, la acción de sus conductores políticos o militares se desordena, se transforma en reacción y la sensación de escasez de tiempo comienza a influir en sus decisiones acelerándolas a tal nivel que no es posible coordinar los esfuerzos ni conducirlos apropiadamente.

La función mando y control, al encargarse de proveer la información que se requiere para la toma de decisiones con la menor incertidumbre posible, se transforma en un objetivo que debe ser atacado o defendido en la guerra de la información. Siendo así, es indudable que la infraestructura que sirve a la función será objeto de acciones ofensivas para restarle capacidades o para neutralizarla con el propósito de impedir que cumpla su propósito. Con lo anterior, el atacante alcanzaría un grado de libertad de acción que le permitirá adelantar su ciclo de decisiones y, a la vez, interferir y quebrar el ciclo de decisiones del adversario, de tal manera que una autoridad política o militar y su respectiva cadena de mando se confunda, paralice y finalmente colapse. Considerando que todo esto ocurre preferentemente en el ciberespacio la acción del atacante se vería facilitada, en tanto que la defensa enfrentaría dificultades para detectar e identificar al atacante, para localizarlo y para intentar su neutralización.

Un ataque a la infraestructura de mando y control dificultaría la conducción de las acciones políticas o militares, más aún si se ha optado por la práctica del mando y control detallado. Si por el contrario, se ha resuelto practicar el mando y control directivo, es probable que los efectos del ataque no permitan que el adversario consiga imponer su voluntad y someter a su oponente con facilidad.

Definitivamente, en el complejo escenario que representa el ciberespacio no solo se llevan a efecto la guerra por la información y el combate por el mando y control, sino que también se genera una lucha por la libertad de acción; y si a ello se le agrega la incertidumbre propia de la guerra y particularmente de la ciberguerra, la complejidad se incrementa dificultando las acciones que deben realizar los conductores políticos y militares para coordinar las capacidades del Estado haciéndolas converger para conseguir la decisión, aplicando el principio de unidad de mando y de esfuerzo.

7 Se está haciendo referencia al centro de gravedad, que al ser atacado de manera exitosa genera la derrota del adversario.

Elementos y amenazas del combate por el mando y control

En el combate (algunos lo denominan guerra) por el mando y control intervienen numerosos elementos, destacando entre ellos: la guerra electrónica, las operaciones de seguridad, las operaciones psicológicas, la decepción y la destrucción física de la infraestructura de información. Este último elemento destaca entre los anteriores porque su aplicación no ocurre solo en el ciberespacio, sino que también puede llevarse a efecto en cualquiera de los otros dominios o escenarios, especialmente en el dominio terrestre.

La guerra electrónica cumple tres tareas que son fundamentales en el combate por el mando y control; la primera de ellas, denominada protección electrónica, consiste en asegurar el empleo del espectro electrónico en beneficio de la acción de mando y control con los medios propios; la segunda tarea, el ataque electrónico, tiene como propósito negar al adversario la capacidad de realizar una acción de mando y control efectivo de sus medios; y, la tercera tarea, apoyo electrónico, es la encargada de proporcionar información en tiempo real, monitoreando al adversario para detectar e impedir el ataque electrónico adversario.

Por su parte, las operaciones de seguridad se orientan a negar la información crítica de las propias capacidades al adversario, de tal manera que este se mantenga en una situación de incertidumbre que dificulte su toma de decisiones o que lo conduzca a resolver erradamente. Para su cometido, las operaciones de seguridad se realizan coordinándolas con las actividades de protección electrónica.

Las operaciones psicológicas, en el caso del combate por el mando y control, se accionan desde el nivel político y estratégico considerando actividades diplomáticas, económicas, militares y de información. Su función se resume en influenciar positivamente el ámbito externo, generar percepciones e inducir el comportamiento en beneficio de las propias metas. Estas operaciones se realizan de manera coordinada con las actividades de protección electrónica y de apoyo electrónico, las que permiten conocer el efecto logrado.

La decepción, por su parte, se orienta a producir una apreciación errónea de la situación propia en el conductor político o militar adversario y sus asesores, de tal manera que su toma de decisiones se dificulte especialmente en situaciones críticas donde el factor tiempo es fundamental. La decepción también se debe coordinar con las actividades de protección y de apoyo electrónico.

La destrucción física de la infraestructura de información adversaria se realiza empleando el armamento aéreo, naval, terrestre o la acción directa de fuerzas de operaciones especiales. Se lleva a efecto después de un riguroso

proceso de selección de objetivos y debe contar con el apoyo de la guerra electrónica, de las operaciones de seguridad y de la decepción.

Otro elemento que aporta sustancialmente en el combate por el mando y control es la Inteligencia, siendo ella la encargada de obtener, analizar, evaluar e interpretar la información relacionada con las capacidades de la infraestructura de mando y control del adversario y con las capacidades del armamento que pudieran afectar la propia capacidad durante el combate por el mando y control. La Inteligencia como función primaria apoya con información referida a los procedimientos, estructura organizacional y estimación de las áreas de despliegue de los sistemas de mando y control adversarios. Simultáneamente, apoya con operaciones de contrainteligencia para proteger la infraestructura de mando y control propia.

En el combate por el mando y control, que se lleva a efecto de preferencia en el ciberespacio, existen amenazas y riesgos que pueden afectar la infraestructura de información pudiendo reducir sus capacidades e inclusive neutralizarlas. La amenaza más presente y de la que existen ejemplos más que suficientes para demostrar su efectividad[8], tanto en el ámbito civil como en el militar, es el ataque cibernético, cuyos efectos van desde interrumpir las comunicaciones de teléfonos móviles hasta impedir el funcionamiento de infraestructura estratégica crítica y que, por supuesto, podrían afectar la infraestructura de mando y control militar. Respecto de esta amenaza, se tiende a pensar que ella es dependiente de la capacidad tecnológica disponible, sin embargo los hechos han demostrado que tecnología suficiente en manos de expertos[9] pueden producir efectos que se traducen en disminución y neutralización de capacidades fundamentales.

Otras amenazas provienen de los elementos del combate por el mando y control del adversario, es decir, de la guerra electrónica, las operaciones de seguridad, las operaciones psicológicas, la decepción y de la capacidad adversaria para destruir físicamente la infraestructura de información propia. Esto implica que para evitar los efectos de dichas amenazas o al menos minimizarlos, es indispensable accionar con anticipación y previsión empleando toda la capacidad propia para proteger las redes e infraestructura de información.

8 Kolton: *La seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización futuras,* p. 55, sostiene que el año 2014, cuando Rusia tomó el control de Crimea se produjo una "interrupción significativa de teléfonos móviles" y que el 23 de diciembre de 2015 un "supuesto ataque cibernético" habría afectado a más de setecientos mil ucranianos al dejarlos sin electricidad. A estos ejemplos se suman otros, como los ciberataques sufridos por Estonia el año 2007, como lo señala Torres en *Ciberguerra,* p. 337.

9 Se está haciendo referencia a los *hackers*, quienes son capaces de penetrar sistemas de alta sofisticación para introducir códigos "malignos", borrar archivos de relevancia o interrumpir el funcionamiento de infraestructura crítica, entre otros.

Es importante considerar que las amenazas provienen de actores estatales y no estatales, a los que se suman organizaciones criminales, amenazas de actores internos e inclusive los errores inconscientes de operadores propios. A estas amenazas se suman los riesgos provenientes de la ausencia de regulaciones y procedimientos para la operación de sistemas, incumplimiento de normas de seguridad, ausencia de programas de seguridad cibernética; desconocimiento o falta de experiencia en la aplicación de regulaciones, procedimientos y programas de seguridad cibernética; y, especialmente, ausencia de políticas, estrategias y directivas operacionales de seguridad cibernética que sean realmente efectivas.

Una de las formas de combatir las amenazas en el combate por el mando y control consiste en alcanzar la "supremacía en el ciberespacio"[10], que es sinónimo del "dominio cibernético" establecido por otros autores. Esto se relaciona con la capacidad de accionar en el ciberespacio conforme con la propia voluntad, de tal manera que se pueda emplear la infraestructura tecnológica de información con el máximo de libertad de acción y seguridad, tanto de manera defensiva como ofensiva. Así la supremacía y el dominio cibernético se relacionan con el poder, adquiriendo la denominación de ciberpoder y siendo conceptualizado como la capacidad de emplear el ciberespacio para generar ventajas, oportunidades y situaciones que influyan decisivamente en otros actores[11].

Para la obtención de la supremacía o dominio cibernético en el ciberespacio es necesario recurrir a las capacidades de la organización, a las estrategias y procedimientos, a la infraestructura tecnológica que interviene en la guerra de información, y a los elementos del combate por el mando y control. Para la obtención del dominio cibernético o supremacía en el ciberespacio se recurre a las capacidades que provienen tanto de la organización, estrategias y procedimientos como de la infraestructura tecnológica que interviene en la guerra de información, es decir, se emplearán las capacidades de operaciones sicológicas, de decepción, de guerra electrónica y de destrucción física de la infraestructura de información del adversario, entre otros.

De lo presentado respecto del propósito de la supremacía cibernética se confirma su estrecha relación con la libertad de acción; primero, porque la libertad de acción favorece el empleo de la propia capacidad cibernética con la menor oposición de un adversario en el ciberespacio; segundo, porque la

[10] Nigel Inkster. *China's Cyber Power,* London: The International Institute for Strategic Studies, 2016, pp. 97-100.

[11] Stuart H Starr. *Developing a theory of Cyberpower en:* Tarek Saadawi y Louis Jordan Jr. *Cyber Infraestructure protection,* Carliste: Strategic Studies Institute, U.S. Army War College, 2011, p. 17.

libertad de acción contribuye a que el empleo de la propia capacidad cibernética sirva a la obtención de la supremacía en el ciberespacio con economía de medios y fortaleciendo la seguridad; y tercero, porque como consecuencia de la obtención de la supremacía en el ciberespacio se consigue la parálisis política, estratégica u operacional del adversario, la que aporta condiciones óptimas para hacer realidad la propia intención. Para la obtención del dominio cibernético o supremacía en el ciberespacio se recurre a las capacidades que provienen tanto de la organización, estrategias y procedimientos como de la infraestructura tecnológica que interviene en la guerra de información, es decir, se emplearán las capacidades de operaciones sicológicas, de decepción, de guerra electrónica y de destrucción física de la infraestructura de información del adversario, entre otros.

Por otra parte, del análisis de la relación entre la supremacía cibernética y el combate por el mando y control se infiere que disponer de la citada supremacía contribuye a que la entrega de la información para la toma de decisiones se produzca con rapidez, oportunidad, mayor grado de certidumbre y, especialmente, con seguridad. Lo anterior se debe a que el adversario no estará en condiciones de oponerse e interferir de manera importante, porque sus capacidades para hacerlo se encontrarán disminuidas o neutralizadas y su actuar no dispondrá de la libertad de acción suficiente para oponerse de manera efectiva. Esta situación contribuirá a que el sistema de mando y control propio adquiera condiciones para fortalecer la unidad de mando y dirección que se requiere para que los esfuerzos confluyan en el punto de la decisión, así como fue planificado y de manera coordinada y segura.

Existe consenso respecto de que el empleo de la asimetría constituye una opción política y estratégica que de ser aplicada podría influir tanto en la libertad de acción como en el esfuerzo para conseguir la supremacía cibernética. Para entender el porqué de lo anterior, es necesario recordar que en situaciones de conflicto internacional la aplicación de la asimetría se evidencia cuando uno de los actores basa su actuar en el empleo de modos diferentes a los de su adversario y el empleo de sus medios se orienta a imponerse a las capacidades superiores de su oponente por medio de lo irregular con fuerte sustento psicológico. Lo anterior, produce un escenario de enfrentamiento extremadamente complejo, con presencia de amenazas difíciles de eliminar, situación que fortalece la sensación de vulnerabilidad y sitúa a los responsables de las decisiones políticas y militares en un ambiente de gran incertidumbre que produce atrición psicológica que puede conducir a la parálisis política y estratégica y, por consiguiente, a la pérdida de la libertad de acción.

El empleo de la asimetría para reducir la libertad de acción de un adversario superior debería orientarse especialmente a neutralizar las capacidades

de mando y control de este, empleando medios reducidos que son capaces de infringir grandes daños de manera imprevista, indirecta y desde posiciones desconocidas y múltiples que dificultan su neutralización o destrucción. Como consecuencia de la degradación de la capacidad de mando y control, es probable que quien toma las decisiones sufra los efectos de la atrición y se vea impedido para continuar conduciendo su accionar con una adecuada coordinación y sincronización de los esfuerzos, porque estará enfrentando niveles altos de incertidumbre debido a que no se puede identificar, localizar, ni atribuir el ataque asimétrico. En el caso de que la acción asimétrica se mantenga es probable que el afectado entre en la condición de parálisis que se mencionó con anterioridad.

El empleo de la asimetría para degradar el sistema de mando y control de un adversario superior puede combinar acciones en el ciberespacio con acciones directas en contra de la infraestructura física que contiene la tecnología de información, es por ello que cuando aparece en el combate por el mando y control la situación se torna más compleja y la incertidumbre se incrementa, pudiendo inhibir la decisión de emplear capacidades superiores, entre ellas las relacionadas con el ciberpoder.

En la búsqueda de la supremacía cibernética también son importantes las aproximaciones que realiza el Ejército de Tierra de Francia respecto del dominio del tiempo y el dominio de la tecnología[12]. Porque el dominio del tiempo se refiere a actuar con urgencia para aplicar la iniciativa que permite obtener libertad de acción para accionar oportunamente y anticipándose al adversario. En el dominio del tiempo son fundamentales las decisiones políticas y militares y, según la doctrina francesa, es probable que ante la presencia de la asimetría, las decisiones militares tengan que adoptarse independientes de las decisiones políticas. Respecto del dominio de la tecnología, lo que sostiene el Ejército de Tierra de Francia es que si se quiere actuar con urgencia, especialmente en un escenario asimétrico, ese dominio se convierte en un multiplicador de eficacia que incrementa el poder, porque permite integrar todo tipo de capacidades, incluidas las cibernéticas relacionadas con la información, optimizando la maniobra política, estratégica u operacional. Además, se sostiene que el dominio del tiempo en conjunto con el dominio de la tecnología contribuyen a disminuir las propias vulnerabilidades, a incrementar la seguridad y a enfrentar amenazas que sufren permanentes transformaciones.

12 Armée de Terre. *Ganar la batalla. Conducir a la Paz,* París: Centre de Doctrine d'Emploi des Forces, 2007, pp. 52-56.

De los planteamientos anteriores se desprende que en el ciberespacio se desarrolla una intensa interacción entre los elementos del combate por el mando y control con las amenazas y riesgos que se manifiestan en ese "quinto dominio". Lo sorprendente es que los mismos elementos del mando y control se transforman en amenazas para el mando contrario, sumándose a otras que se han identificado en esta parte del presente artículo. En igual sentido, llama la atención que muchos de los riesgos ya citados guardan relación con acciones u omisiones propias; y que la acción asimétrica debe ser considerada una amenaza. Frente a lo anterior, la solución parece ser alcanzar la supremacía cibernética, lo que implicaría la ejecución de acciones ofensivas y defensivas acompañadas por un permanente desarrollo tecnológico para asegurar la superioridad.

La disputa por el mando y control

La revisión y análisis realizados en los acápites anteriores contribuyen a demostrar la existencia de una disputa por el mando y control en el ciberespacio y también en los otros dominios, es decir, en lo terrestre, en lo naval, en lo aéreo y en lo espacial. También ha quedado en evidencia que dicha disputa incrementa progresivamente su complejidad e importancia, presentando la característica de un verdadero combate para conseguir la supremacía de mando y control y de esa manera poder imponerse al adversario.

Se entiende que la superioridad en mando y control impacta decisivamente en la lucha para obtener la libertad de acción y que esta, a la vez, repercute en la práctica de la unidad de mando que facilita la convergencia de los esfuerzos políticos y estratégicos, incluyendo entre los últimos a los esfuerzos militares. Se suma a lo anterior, que la victoria en la lucha por el mando y control contribuye al logro de la supremacía cibernética que, aunque sea temporal, incrementará los niveles de libertad de acción y la seguridad de quien esté en posesión de ella, facilitándole la toma de decisiones y su accionar posterior sin mayores interferencias por parte del adversario.

El combate para obtener la superioridad de mando y control requiere contar con un sistema que para estos fines sea robusto y resiliente, es decir, que por una parte tenga mayores capacidades que las del adversario para no transformarse en objetivo de su acción cibernética y menos aún de sus ataques por la vía convencional; y que por otra parte, sea capaz de resistir y de recuperarse con rapidez de los efectos provocados por eventuales ataques exitosos que provengan del mencionado adversario. Lo anterior, también se relaciona directamente con las amenazas que están presentes en el ciberespacio

y, además, con aquellas que provienen de la capacidad de destrucción física de la infraestructura de mando y control por parte del adversario.

Una de las mayores dificultades para desarrollar el combate por el mando y control cuando este ocurre en el ciberespacio, radica en la dificultad que existe para localizar geográficamente el origen del ataque debido a que regularmente este no "siempre deja tras de sí una estela que pueda ser rastreada"[13], lo que prácticamente impide identificar al responsable y, por consiguiente, dificulta y puede impedir la planificación y ejecución de algún tipo de respuesta. Al respecto, cuando el ataque responde a la propia intención lo anterior constituye una ventaja, pero cuando proviene del adversario se transforma en dificultad e inclusive en incapacidad para responder a la agresión.

Otro asunto importante en el combate por el mando y control se refiere a la permanencia de los efectos, asunto que deriva de la fortaleza y capacidad de resiliencia de las estructuras. Esto ha generado un planteamiento en donde se asume que una acción ofensiva exitosa contra la estructura de mando y control del adversario solo produciría una superioridad temporal y no absoluta, generando una ganancia en cuanto a libertad de acción que debe ser explotada con rapidez para no perder la oportunidad y la ventaja que se consiguió. Es aquí donde cobra importancia la aplicación del modelo de mando y control directivo, porque en las condiciones descritas no se dispondrá del tiempo necesario para emitir documentos ejecutivos detallados, tampoco para controlar los que elaboren los escalones subordinados y, menos aún, para controlar su ejecución. Lo anterior, constituye un desafío porque implica haber desarrollado niveles de confianza que favorezcan la entrega de facultades para que los mandos subordinados puedan aplicar su iniciativa y accionar con mayor independencia, practicando el ya conocido mando tipo misión.

Otro desafío radica en la generación de capacidades para que el combate por el mando y control conduzca a la victoria, debido a que por una parte existe la necesidad de contar con un sistema robusto y resiliente que resulte de la integración de todas las capacidades disponibles, es decir, tanto las civiles como las militares y, entre estas últimas, las que provengan de las diferentes instituciones de la defensa nacional; y por otra parte, se manifiesta la necesidad de emplear sinérgicamente las capacidades de mando y control, lo que implica procedimientos comunes, entrenamiento certificado, coordinaciones y sincronización de esfuerzos con el objeto de evitar interferencias,

[13] Torres: *Ciberguerra*, pp. 333-334. Torres denomina a esto "los problemas de atribución" señalando, además, que se debe a que los ataques pueden proceder "de diferentes puntos del planeta".

economizar medios y conseguir la unidad de mando y con ella la convergencia de los esfuerzos.

En la práctica, el combate por el mando y control significa inutilizar los sistemas del adversario, lo que requiere conocer con anticipación las vulnerabilidades de dichos sistemas demandando un tremendo esfuerzo de búsqueda para obtener la información necesaria. Al respecto, es indispensable que esa información se obtenga en tiempos de normalidad, explotando las oportunidades que se presentan cuando no existe conflicto o la intensidad de este es baja y los niveles de seguridad tienden a reducirse. En esta tarea, son los propios sistemas de mando y control, sumados a la capacidad de guerra electrónica, como uno de los elementos del combate por el mando y control[14], sumados al apoyo de la Inteligencia[15], los que pueden contribuir al descubrimiento de las citadas vulnerabilidades.

El secreto constituye un asunto fundamental en el combate por el mando y control porque consiste en impedir que el adversario conozca la propia infraestructura, menos aún que obtenga conocimiento de las vulnerabilidades que esta pueda presentar. Para esto es indispensable que las operaciones de seguridad propia sean efectivas y puedan negar la información crítica. Lo anterior puede ser más efectivo aún si es que se combinan con operaciones de decepción que conduzcan al adversario a una apreciación errada de las propias capacidades; y, también, si es que se combinan con acciones de protección electrónica que dificulten el empleo del espectro electrónico por parte del adversario. Si la mantención del secreto es exitosa, simultáneamente se generará la sorpresa que potenciará el accionar propio asegurando la supervivencia de los medios empleados.

Un asunto que no puede dejar de mencionarse se refiere a que aún cuando el combate por el mando y control se desarrolla preferentemente en el ciberespacio, siempre existirá el riesgo de que parte importante de la infraestructura (de mando y control) pueda ser neutralizada o destruida en su despliegue terrestre, mediante el ataque con armamento de precisión operado desde largas distancias o mediante la acción directa de fuerzas de operaciones especiales, inclusive por el empleo de actores asimétricos que puedan ser reclutados para esos fines.

14 Se refiere a la guerra electrónica que cumple la tarea de proporcionar información monitoreando al adversario para detectar e impedir un ataque electrónico de su parte.

15 Recordar que la Inteligencia es la encargada de obtener, analizar, evaluar e interpretar la información relacionada con las capacidades de la infraestructura de mando y control del adversario, incluyendo las capacidades del armamento que pudiera ser empleado en contra de la propia capacidad.

Cuando se esté combatiendo por el mando y control el dominio de la tecnología será un elemento fundamental para dominar el tiempo y de esa manera poder actuar con la rapidez necesaria para anticiparse al accionar del adversario. Esto constituye un desafío que impacta en el elemento humano, porque lo obliga a estar familiarizado con dicha tecnología, a entrenarse y a ser capaz de explotar al máximo sus capacidades, lo que implica altos niveles de capacitación y entrenamiento permanente. Se asocia a este desafío la necesidad de contar con el sostenimiento suficiente para que la infraestructura de mando y control se mantenga permanentemente operacional. Esto último requiere integrar las capacidades civiles y militares por medio de alianzas públicas y privadas para desarrollar tecnología, apoyar su operacionalidad e inclusive para contribuir a su protección, entre otros asuntos.

Un asunto que podría influir negativamente en el combate por el mando y control es el exceso de burocracia practicado especialmente en los procedimientos de transmisión de tareas, en la transmisión de información y en los procedimientos de control, porque ello impacta negativamente en los esfuerzos para conseguir el dominio del tiempo, actuar con rapidez y para anticiparse al adversario. Al respecto, se debe considerar que la superioridad cibernética es temporal y difícilmente absoluta, por tanto la rapidez se convierte en un requisito fundamental y la burocracia excesiva actúa en su contra.

La trascendencia, importancia y el carácter evolutivo del combate por el mando y control conducen a formular una estrategia que facilite la preparación, ejecución y la dirección de los esfuerzos para alcanzar los efectos deseados y conseguir la victoria en el ciberespacio, considerando que esa victoria beneficiará a la toma de decisiones por parte de líderes políticos y militares y será fundamental para la conducción de los esfuerzos en procura de los objetivos propuestos, permitiendo accionar con el máximo de libertad de acción, asegurando la unidad de mando y la convergencia de los esfuerzos políticos y estratégicos. El propósito de la citada estrategia debería orientarse a la disuasión del adversario, a conseguir la supremacía en el ciberespacio y a paralizar el accionar del adversario. Los mayores desafíos de la citada estrategia se relacionan con ganar la lucha por la libertad de acción, asumir la modalidad directiva del mando y control y a vencer las amenazas y riesgos que se manifiesten en el ciberespacio y en los otros dominios en que se encuentre desplegada la estructura de mando y control propia. Al mismo tiempo, la estrategia debería considerar lo necesario para impedir que el adversario pueda actuar empleando sus propias capacidades de mando y control, siendo este el fundamento que respalda la necesidad permanente de anticiparse a las decisiones adversarias y de actuar con rapidez y con el máximo dominio del tiempo.

Lo expuesto en los párrafos precedentes permite identificar algunos objetivos que debe contener una estrategia para el combate por el mando y control, entre ellos los siguientes:

- Potenciar las capacidades de mando y control mediante herramientas de detección, prevención y de defensa.
- Desarrollar capacidades de respuesta efectiva a los ataques adversarios.
- Consolidar el empleo seguro de la propia capacidad de mando y control para vencer en la guerra por la información.
- Potenciar la estructura de mando y control desarrollando un alto nivel de resiliencia.
- Capacitar y entrenar al elemento humano de la estructura de mando y control para dominar la tecnología, dominar el tiempo y ganar la iniciativa.
- Asegurar la utilización del mando y control directivo y el mando tipo misión.
- Generar la cooperación civil, militar, pública y privada para contribuir al sostenimiento de la infraestructura de mando y control.
- Contribuir a la obtención de la victoria en la guerra por la información.

Es importante considerar que la victoria en el combate por el mando y control sirve a la configuración del campo de batalla y que también puede contribuir a que la disuasión sea creíble en los términos que lo señala Beaufre[16]. Respecto del aporte para la configuración del campo de batalla, ello se consigue alcanzando la supremacía en el ciberespacio y venciendo al adversario en la lucha por la libertad de acción, porque lo obliga a tener que reaccionar permanentemente, disponiendo de escasa capacidad para accionar conforme a sus intenciones. En relación con la disuasión, la supremacía en el ciberespacio facilita el desarrollo de acciones que demuestren el ciberpoder alcanzado y la voluntad para emplearlo de manera ofensiva si es que ello fuera necesario. Como se puede apreciar, el aporte a la configuración del campo de batalla, que también puede aplicarse al escenario de conflicto y crisis, radica en la demostración de capacidad y en la advertencia, que en conjunto incrementan la incertidumbre dificultando y retardando la toma de decisiones.

16 Beaufre sostiene que para evitar "una prueba de fuerza" con el adversario es necesario disponer de una fuerza ofensiva que lo desanime a emplear la suya. En el caso de combate por el mando y control correspondería a una estructura con gran capacidad de penetración, de precisión y de destrucción.

Reflexiones finales

Así hemos podido establecer el cómo alcanzar la victoria en el combate por el mando y control, asumiendo como constante que dicho combate se lleva a efecto principalmente en el ciberespacio, pero sin que ello signifique que en el resto de los dominios, particularmente en el terrestre, nada ocurre. También se consideró que el citado combate se relaciona estrechamente con la guerra por la información y que sus acciones son tanto de carácter defensivo como ofensivo.

En la primera parte de esta reseña se profundizó el conocimiento respecto de la relación que existe entre la guerra de información y el mando y control en el ciberespacio, pudiendo establecerse que dicha relación gira en torno a la existencia de un tercer elemento, que influye notoriamente en el análisis y que se refiere a la necesidad de generar libertad de acción para fortalecer la unidad de mando y contribuir a la convergencia de los esfuerzos políticos y estratégicos y, finalmente, conseguir el o los objetivos propuestos. Además, se consideró que todo ello, por el hecho de ocurrir en el ciberespacio, adquiere una connotación especial, debido al factor tiempo que obliga a conseguir los estados deseados con rapidez para así mantener la iniciativa.

En la segunda parte se revisaron los elementos del combate por el mando y control y se identificaron las amenazas que se manifiestan durante la ejecución de dicho combate en el ciberpacio y en el dominio terrestre. En este segmento se analizó la interacción que se producen entre ambos, pudiendo determinarse que los elementos y amenazas son comunes para los actores en conflicto y que el dominio del tiempo es determinante para anticiparse a las intenciones de cada uno, para ganar la iniciativa y obtener la libertad de acción que se requiere para accionar con el mínimo de interferencia u oposición.

En la tercera parte se identificaron y analizaron los desafíos y las condiciones que demanda alcanzar la victoria en el combate por el mando y control, junto con ello se pudo establecer que para conseguir la supremacía cibernética es indispensable contar con una infraestructura de mando y control robusta y altamente resiliente, de tal manera que sus capacidades sean superiores a la del adversario. También se estableció que en el combate que se lleva a efecto en el ciberespacio es muy difícil identificar al atacante y localizar geográficamente el origen de un ataque, lo que, en conjunto, dificulta ejecutar una represalia. Además, surgió un asunto que es relevante al momento de evaluar los efectos de una acción ofensiva exitosa en el ciberespacio, porque dichos efectos son temporales y no absolutos debido a la robustez y resiliencia de las estructuras de mando y control, situación que obliga a actuar con rapidez para explotar el éxito. En esta parte también se identificaron y analizaron otras condiciones y desafíos de vital importancia en el combate por el mando

y control, así como asegurar el secreto, desarrollar y dominar la tecnología, asegurar el sostenimiento de la infraestructura, emplear sinérgicamente las capacidades disponibles, evitar la burocracia excesiva e integrar las capacidades civiles y militares relacionadas con el asunto en estudio.

Antes de finalizar la tercera parte de este título se analizó la necesidad e importancia de contar con una estrategia orientada a combatir con éxito por el mando y control y como consecuencia alcanzar la victoria en el ciberespacio. Allí, junto con señalar el propósito general de la estrategia, se formularon algunos de los objetivos que podría contener, los cuales tendrían que generar líneas de acción referidas a capacidades, seguridad, resiliencia, cultura de ciberseguridad para el mando y control y, especialmente, relacionadas con la generación de compromiso hasta el nivel del Estado.

Lo anterior demuestra que aquel que sea capaz de accionar contra su adversario, amparado en el secreto y desde largas distancias, tendrá la capacidad de dañar y neutralizar su infraestructura de mando y control sin necesidad de comprometer medios humanos y materiales, lo que le permitirá realizar economía de fuerzas y conseguir su propósito con mayor rapidez. Esto mismo permitirá configurar un escenario político y estratégico y, de ser necesario, un campo de batalla favorable para continuar sus acciones y conseguir su propósito final. También será capaz de vencer a su adversario en la guerra por la información y por consiguiente poseerá la supremacía cibernética y el control del ciberespacio. No poseer la capacidad para vencer en el combate por el mando y control significa estar dispuesto a perder la libertad de acción y con ello someterse a la voluntad de un adversario.

Conseguir libertad de acción en un dominio como el ciberespacio, donde el adversario puede ejercer algún grado de control, es tremendamente difícil y requiere alta disponibilidad de tecnología avanzada de mando y control, para asegurar la obtención y entrega de información y para apoyar el control directivo de los esfuerzos, conforme con las exigencias que los escenarios políticos y estratégicos actuales imponen, considerando, además, que los nuevos escenarios podrían exigir mayores capacidades en el futuro.

Para conseguir la supremacía cibernética es indispensable desarrollar y emplear efectivamente el ciberpoder, enfrentando amenazas complejas y de gran potencialidad, conforme con lo establecido en una estrategia de acción en la que se reúnen capacidades civiles y militares. Esto implica que el combate por el mando y control no constituye un asunto exclusivamente militar, sino que constituye un desafío del Estado en general, porque los resultados favorecerán o afectarán tanto la toma de decisiones políticas como las militares.

Lo tratado y propuesto no agota el tema, será necesario continuar la investigación y reflexionar profundamente respecto de los desafíos que provengan de las demandas de los nuevos escenarios políticos y estratégicos, los

que, seguramente, exigirán nuevas capacidades para combatir por el mando y control, para obtener la victoria en la guerra por la información y para ganar la libertad de acción.

Bibliografía

Armée de Terre. *Ganar la batalla. Conducir a la Paz.* París: Centre de Doctrine d'Emploi des Forces, 2007.

Beaufre, Andre. *Introducción a la Estrategia.* Madrid: Instituto de Estudios Políticos, 1965.

Department of the Army. *FM 3-12 Cyberspace and electronic warfare operations.* Washington D.C., 2017.

Dunivan, Jim. *C2 en el campo de batalla digitalizado: ¿Cediendo la iniciativa?,* en Military Review. Kansas, Fort Leavenworth: 2004.

Graham, Matt. *La fuerza cibernética de EUA,* en Military Review. Kansas, Fort Leavenworth: Centro de Armas Combinadas, julio-septiembre 2016.

Inkster, Nigel. *China's Cyber Power.* London: The International Institute for Strategic Studies, 2016.

Joint Staff Pentagon. *Joint Pub 3-13.1. Joint Doctrine for Command and Control Warfare (C2W).* Washington D.C., 1996.

Joint Staff Pentagon. *Joint Pubblication 3-12 (R). Cyberspace Operations.* Washington D.C., 2013.

Jordán, Javier y Baqués, Josep. *Guerra de drones: Política, tecnología y cambio social en los nuevos conflictos.* Madrid: Editorial Biblioteca Nueva S.L., 2014.

Klimburg, Alexander y Hathaway, Melissa E. *National Cyber Security.* Tallin, Estonia: NATO CCD COE Publications, 2012.

Kolton, Michael. *La seguridad cibernética de las naciones anfitrionas en las operaciones de estabilización futuras,* en Military Review. Kansas, Fort Leavenworth: Centro de Armas Combinadas, mayo-junio 2016.

Starr, Stuart H. *Developing a theory of Cyberpower,* en Saadawi, Tarek y Jordan, Louis: *Cyber Infraestructure Protection.* Carliste: Strategic Studies Institute, U.S Army War College, 2011.

Torres, Manuel R. *Ciberguerra,* en Jordan, Javier: *Manual de Estudios Estratégicos y Seguridad Internacional.* Madrid: Plaza y Valdés S.L., 2013.

Wendt, Alexander. *Social Theory of International Politics.* Cambridge: Cambridge University Press, 2006.

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 tácticos[2], 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 misión[3].

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 riegos 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 espionaje[4], 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 Defensa, UK, 2016, pp. 19-33.

propiamente 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 nacional[5]. 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 Nº 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 inversores[6]. 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 políticas[7].

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 ámbitos[8]. 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 Ibíd., 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 Canadá[12], 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 infraestructures: 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 Nº 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 operacionalidad 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 enemigo[15]. 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 grande[16]. 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, interdictar, 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 Nº 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 existentes[17].

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 Ucrania[18], 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 infraestructures 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 internacional[19]. 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 política[20].

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 Ibíd., 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 atribución[21], 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 un 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] Ibíd., 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. Distraer, 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 efectué 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 organización 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 nacional[24].

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 Nº 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 "afrontarlas 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 ciberguerra[25]. 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 continental[26].

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 Nº 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 bajó 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 la 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 operacionalidad 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 Nº 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 Nº 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 iniciates 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 Parlament, 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 Nº 185, Ciberseguridad, la cooperación público-privada, España, 2016.

Johnson, Thomas. Cybersecutity protecting critical infraestructures 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 Nº 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.

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.

Capítulo 6

El Derecho Internacional como marco regulatorio de la ciberguerra

Mario Polloni Contardo[*]

Introducción

El propósito de este capítulo es presentar de una manera ordenada cómo y con qué extensión el Derecho Internacional regula las acciones desarrolladas por diversos actores en el marco de la llamada "ciberguerra". Un primer punto a tratar en este esfuerzo se orienta a distinguir el concepto de ciberguerra respecto de otros que, no obstante perteneciendo a un mismo género, responden a parámetros más amplios y a una naturaleza distinta del que restrictivamente se aplica en el entorno de conflicto armado, y por esta razón a la ciberguerra. Esta distinción se realiza solo en términos descriptivos, toda vez que su intención es dar un contexto a lo esencial del trabajo. Luego se avanza en la presentación de consideraciones y esfuerzos a nivel internacional para desarrollar políticas y cuerpos normativos –en general escasos– que orienten y regulen el uso pacífico del espacio cibernético y lo resguarden de su uso ilegal. A continuación se identifica el marco regulatorio de la ciberguerra en dos dimensiones. La primera está relacionada con el campo propio del *jus ad bellum*, es decir, las condiciones exigidas por el Derecho para que los recursos de la ciberguerra se empleen como medios y métodos de guerra en el contexto de un conflicto armado, y dentro de los cauces permitidos por el orden jurídico; la segunda de estas dimensiones

[*] Mario Polloni Contardo es Teniente Coronel (R) del Ejército de Chile. Oficial de Estado Mayor, Abogado, Pontificia Universidad Católica de Chile, Magíster en Asuntos de Seguridad Nacional, Colegio Naval de Postgrado de Monterrey, EE.UU., Magíster en Derecho Constitucional, Universidad de Talca.

tiene que ver con el *jus in bello*, el cómo se emplean estos recursos en el transcurso del conficto, teniendo siempre en vista el recaudo de bienes jurídicos, sociales y humanitarios que, no importando las causas que llevan a los Estados y actores al uso de la fuerza como medio de resolución de conflictos, deben ser protegidos a todo evento.

En lo particular, el trabajo en su parte final describe los aspectos esenciales del Manual de Tallinn, texto que, como se explicará, constituye el mayor esfuerzo para establecer reglas no vinculantes que establecen el marco para el uso de medios y métodos de ciberguerra en conflictos armados.

De esta manera se pretende dar respuesta a dos preguntas que constituyen imperativos que orientan este trabajo:

¿Qué regulaciones desde el punto de vista jurídico contempla la ciberguerra?

¿Qué consideraciones regulatorias contiene el DICA respecto de la ciberguerra?

Marco conceptual

La ciberguerra se enmarca en el concepto global de ciberseguridad, constituyendo una parte o especie de esta última. La ciberseguridad está orientada a establecer estructuras, procedimientos y mecanismos que permitan, en tiempo de paz y de conflictos, el uso del espacio para fines de desarrollo, a nivel individual como social. En este sentido, los Estados elaboran políticas de ciberseguridad que persiguen estos fines.

En el caso de Chile, la Política Nacional de Ciberseguridad declara como propósitos los siguientes:

- Resguardar la seguridad de las personas en el ciberespacio.
- Proteger la seguridad del país.
- Promover la colaboración y coordinación entre instituciones.
- Gestionar los riesgos del ciberespacio.

Afirma la Política Nacional de Ciberseguridad de Chile que "atendido el carácter global del ciberespacio, los riesgos y amenazas provienen de Chile y del exterior y se originan tanto en causas naturales como en actividades delictuales, por ejemplo, en labores de espionaje y vigilancia llevadas a cabo con diversos fines, afectando la confidencialidad, integridad, disponibilidad de los archivos de información en el ciberespacio, y con ello, los derechos de las personas"[1].

[1] Gobierno de Chile, *Política Nacional de Ciberseguridad 2017-2022,* p. 12.

Del concepto de ciberseguridad, es posible distinguir diversos tipos de amenazas que afectan el uso tranquilo del ciberespacio, que son el cibercrimen, el ciberterrorismo y la ciberguerra[2].

La ciberguerra, tema de interés para este trabajo, se puede definir como "conflicto entre Estados tecnológicamente avanzados, que se realiza mediante ciberataques aisladamente, o como parte de una guerra convencional. No obstante los conflictos y confrontaciones en el ciberespacio pueden no ocurrir en el contexto de una guerra ni en una confrontación general… [corresponde al] conjunto de acciones que se realizan para producir alteraciones en la información y en los sistemas del enemigo, a la vez que se protegen la información y los sistemas del atacante"[3].

Respecto del concepto de ciberguerra, es pertinente afirmar que en esta dimensión "…no es fundamental ni el tiempo, ni el espacio, ni el clima, ni el arsenal, ni el número de tropas, ni la movilización, ni las pérdidas de vidas humanas…el factor central de la ciberguerra radica en encontrar brechas de seguridad para afectar las redes de información y comunicación de otros Estados. Los ataques cibernéticos capitalizan las debilidades que tiene el sistema informático para extraer información estratégica o boicotear procesos vitales para la nación"[4].

Ciberguerra y Defensa

En un interesante trabajo, el investigador Victor Luke desarrolla aspectos que vinculan la infraestructura crítica de orden informática con la necesidad de preservar y defender esta infraestructura de ciberataques, tema que conduce a la ciberguerra como objeto de estudio desde la perspectiva del Derecho[5].

Desde el punto de vista de la infraestructura crítica, señala Luke que "…El satisfactorio funcionamiento de una sociedad moderna supone el eficiente desempeño de una serie de elementos tangibles e intangibles denominada *infraestructura crítica.* Este es un complejo sistema compuesto de

2 Jesús Reguera Sánchez, *Aspectos Legales en el Ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario,* Grupo de Estudios en Seguridad Internacional, GESI, Universidad de Granada, p. 3.

3 Op. cit. Jesús Reguera Sánchez, *Aspectos Legales en el Ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario,* p. 4.

4 Andrés Gaitán Rodríguez, *El Ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI,* Bogotá, Escuela Superior de Guerra de Colombia, 2012, p. 30.

5 Víctor Luke. Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas. *Revista de Derecho Público, 0* (77), 2012, pp. 405-424. doi:10.5354/0719-5249.2012.30935

mecanismos, servicios, agencias, entes y bienes presentes en un país e incluso, dependiente de factores y elementos ubicados fuera de sus fronteras físicas. Esto hace de la *infraestructura crítica* una compleja red, cuyo comportamiento es difícil analizar y más aun prever"[6]. Agrega Luke que la razón básica que vincula a la Defensa Nacional con la protección de la infraestructura informática de un país radica en que la dependencia tecnológica abre un flanco de vulnerabilidad de enorme envergadura para todo el Estado; y esa vulnerabilidad se acentúa debido a la consolidación de la ciberguerra como una amenaza real a la seguridad de los Estados en el siglo XXI[7]. En este sentido, este autor concluye citando a la revista *Neewsweek Magazine*, "El peligro de un ciberataque es en la actualidad ampliamente reconocido por las sociedades avanzadas, las cuales son completamente dependientes de redes computacionales tanto para el funcionamiento del día a día como para la defensa nacional"[8].

De ahí que se haga necesaria la protección de aquellos "medios electrónicos, que sin ocupar un espacio físico, constituyen el terreno a través del que fluye una creciente cantidad de datos que incluso pueden controlar procesos físicos"[9]. Es por estos medios electrónicos que la ciberguerra y las armas informáticas dirigen su amenaza[10]. Por lo señalado, "las defensas apropiadas para este tipo de amenazas no son las armas convencionales sino las informáticas[11].

Estas consideraciones llevan a Luke afirmar que "…continuar concibiendo a la defensa nacional como una fuerza basada en la posesión de medios disuasivos de carácter físico es mantener una actitud anacrónica. Esto cobra especial relevancia frente a la aparición de amenazas que utilizan armas inmateriales, que se valen de defensas inéditas y que se despliegan en un campo de batalla virtual"[12].

6 Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 409.

7 Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 410.

8 Ibíd.

9 Ibíd.

10 Ibíd.

11 Ibíd.

12 Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 411.

Políticas y marco regulatorio del ciberespacio

El interés por establecer políticas y normas que regulen el uso del ciberespacio y aseguren la seguridad de la información se evidencia con claridad en la década de los 90, y se expresa en la presentación de la Federación Rusa de un proyecto de Resolución (A/RES/53/70) en la Primera Comisión de la Asamblea General de las Naciones Unidas, lo que generó en su momento la conformación del grupo de expertos gubernamentales, con integrantes de Estados Unidos, Rusia y China. A partir de esa fecha, y con mayor fuerza durante la última década, organizaciones regionales como la Organización del Tratado del Atlántico Norte (OTAN) y la Unión Europea han desarrollado iniciativas en términos de políticas y normas para asegurar un uso pacífico o regulado, en el caso de conflictos armados (*jus ad bellum, jus in bello*), del cibersepacio.

En este contexto, con ocasión del 72° período de sesiones de la Asamblea General de Naciones Unidas[13], celebrado durante septiembre de 2017, el ministro de Relaciones Exteriores de la Federación Rusa, Sergei Lavrov, planteó en su discurso ante la Asamblea General la existencia de un vacío de políticas y de normas en materia ciberespacial[14]. En este tema, llamó a rechazar la militarización del ciberespacio; a no permitir que este se convierta en una esfera de confrontación política, y a evitar que se use para infringir presión o daño económico, como diseminar el extremismo e ideologías terroristas. Para avanzar en esos esfuerzos, el canciller llamó a las Naciones Unidas a establecer normas de interés para todos los Estados y de comportamiento responsable en la esfera digital. Concluyó esta autoridad anunciando la preparación de un borrador de una convención universal de lucha contra el crimen cibernético, proponiendo que se comience a revisar en el actual período de sesiones[15].

La exposición del canciller de la Federación Rusa pone en evidencia el vacío normativo internacional en materia de uso pacífico del ciberespacio; por lo que, como se señaló, urge una regulación que satisfaga esta necesidad. Como parte de esta urgencia se inscriben las normas relacionadas con ciberseguridad, ciberdefensa y ciberguerra.

13 Naciones Unidas, Asamblea General, septuagésimo segundo período ordinario de sesiones de la Asamblea General, acceso a Internet el 25 de septiembre, http://www.un.org/es/ga/72/agenda/index.shtml

14 Naciones Unidas, Asamblea General, septuagésimo segundo período ordinario de sesiones de la Asamblea General, discurso del Ministro de Relaciones Exteriores de la Federación Rusa, Sergéi Lavrov, acceso a Internet el 25 de septiembre, , https://www.youtube.com/watch?v=jfMTKr7SGEk

15 Ibíd.

Asimismo, a nivel regional se destaca la existencia de esfuerzos para concordar en políticas y medidas que abordan esta temática en el ámbito de la ciberdefensa. En este contexto, en un ensayo presentado en el VII Congreso del Instituto de Relaciones Internacionales, celebrado en La Plata, República Argentina, entre el 26 y 28 de noviembre de 2014[16], la profesora Candela Justribó expone un estado de situación regional en materia de ciberseguridad y ciberdefensa, Como lo establece la autora, el propósito de su ensayo es "…poder reflexionar y analizar la posibilidad de unificar criterios y lineamientos en torno al rol del Instrumento Militar con respecto a la defensa en el ciberespacio dentro del ámbito de la Unión de Naciones Suramericanas (UNASUR), y su Consejo de Defensa Suramericano"[17].

En el marco señalado, la autora expone que el Plan de Acción correspondiente al 2012 incluyó la conformación de un Grupo de Trabajo para evaluar la factibilidad de establecer políticas y mecanismos regionales para hacer frente a las amenazas cibernéticas o informáticas en el ámbito de la defensa. En esa línea, el Plan de Acción del 2013, también en el eje de "Políticas de Defensa", postuló como actividad a desarrollar el mantenimiento del grupo de trabajo creado el 2012 con el fin de que existiera la posibilidad de "establecer una política y mecanismos regionales para hacer frente a las amenazas cibernéticas e informáticas en el ámbito de la defensa"[18].

Afirma la profesora Justribó que en el marco de la VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado y de Gobierno de UNASUR, celebrada en Paramaribo, República de Suriname, el 30 de agosto de 2013, se acordó instruir al "Consejo de Defensa Suramericano y al Consejo Suramericano de Infraestructura y Planeamiento (COSIPLAN) a evaluar la cooperación con otros consejos ministeriales competentes y avanzar en sus respectivos proyectos de defensa cibernética y la interconexión entre redes de fibra óptica en nuestros países con vistas a tornar más seguras nuestras telecomunicaciones"[19].

Como resultado de lo anterior, en el marco del Consejo de Defensa Suramericano, las ministras y ministros de Defensa retomaron lo expuesto en Paramaribo y revalidaron lo anunciado por ellos en torno a las amenazas cibernéticas e informáticas. En este sentido, ratificaron la necesidad de avanzar en las coordinaciones regionales en materia de ciberdefensa y aprobaron el Plan de Acción del año 2014, en donde por primera vez se incluyó una

16 Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* ensayo presentado en el VII Congreso del Instituto de Relaciones Internacionales, La Plata, Argentina, 26.27 y 28 de noviembre de 2014.

17 Op. cit., Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* p. 1.

18 Op. cit., Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* pp. 3-4.

19 UNASUR, VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado, Declaración de Paramaribo, numeral 29.

actividad didáctica concerniente a la defensa cibernética y respondiendo a la instrucción de la Declaración de Paramaribo, siendo esta un Seminario Regional de Ciberdefensa[20].

Unido a lo anterior, se conformó la segunda reunión del Grupo de Trabajo de Ciberdefensa (Argentina-Perú-Ecuador), mayo 2017, en el marco del Consejo de Defensa Suramericano, cuyo resultado se resume en cuatro puntos[21].

- Crear un foro regional del grupo de trabajo de ciberdefensa de los Estados miembros, con el fin de intercambiar conocimientos, experiencias y procedimientos de solución.
- Establecer una red de contactos de autoridades competentes para el intercambio de información y colaboración de manera permanente.
- Definir la plataforma y procedimientos de comunicaciones de la red de contactos.
- Profundizar y sistematizar la reflexión acerca de definiciones conceptuales de ciberdefensa y ciberseguridad (Declaración de Cartagena del Consejo de Defensa Suramericano, 2014).

Por último, siempre en el marco regional (UNASUR), el 7 de marzo de 2017 se llevó a efecto la 1ª Reunión Virtual del grupo de trabajo de ciberdefensa (Chile-Ecuador-Perú), con el objeto de "…coordinar los esfuerzos de los Ministerios de Defensa de Chile, Perú y Ecuador para establecer principios compartidos de armonización de criterios, definiciones y estrategias que permitan desarrollar una política de ciberdefensa"[22].

El Derecho y la ciberguerra

Ante la falta de normativa expresa en ciberseguridad, una pregunta que surge en el tema es qué normativa es aplicable a la ciberguerra. Esta pregunta es válida tanto para el ámbito del *jus ad bellum* como en el del *jus in bello.*

En el marco del *jus ad bellum* es posible identificar tres aproximaciones para definir cuándo un ciberataque puede ser calificado como un acto de guerra, por tanto de ciberguerra, y objeto de respuesta legal en el marco de un

20 Op. cit., Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* p. 4.
21 Ibíd.
22 UNASUR, Consejo de Defensa Suramericano, Acta 1ª Reunión Virtual Grupo de trabajo Ciberdefensa CDS-UNASUR, de 7 de marzo de 2017, p. 1.

conflicto armado[23]. La primera es la aproximación universal. Lo más cercano es cuando Naciones Unidas declara una acción cibernética como constituyente de un acto de guerra. La dificultad para llegar a esta declaración es que Naciones Unidas no la ha realizado a la fecha y no existe un tratado universal que diga algo más al respecto. Ante esta situación, es complejo declarar un ciberataque como un acto de guerra[24]. La segunda aproximación es la que define un conjunto de Estados reunidos en una organización, como la que puede realizar la Organización del Tratado del Atlántico Norte (OTAN), pero esta declaración y la consiguiente acción para enfrentarla no ha ocurrido, y pudo haber sido esta la ocasión en el ciberataque a Estonia (2007). De haber reaccionado la OTAN al ciberataque de Estonia por considerarlo ilegal, pudo haber originado una respuesta del atacante según sus propios intereses[25]. La tercera aproximación es la unilateral; un Estado puede declarar que un ciberataque de ciertas características es un acto de guerra, y reaccionar con una respuesta en la misma línea. Si un Estado responde al ciberataque en el contexto de un acto de guerra, se podrá considerar esta como una respuesta legal o no, dependiendo si esta emplea una misma o diferente modalidad de ataque. En todo caso, nada obliga a un Estado a considerar el ciberataque como un acto de guerra[26].

En el marco del *jus in bello*, por su parte el Comité Internacional de la Cruz Roja (CICR) entrega una respuesta más precisa. Si se habla de una ciberguerra (entiéndase ataques informáticos dentro de un conflicto armado) establece el CICR que se debe aplicar la normativa del Derecho Internacional Humanitario; según Cordula Droege (2011), asesora legal del CICR, "El Derecho Internacional Humanitario o DIH solo entra en juego si las operaciones cibernéticas se cometen en el contexto de un conflicto armado, sea entre Estados, entre Estados y grupos armados organizados, o entre grupos armados organizados. Por ende, es preciso distinguir la cuestión general de seguridad cibernética, de la cuestión específica que representan las operaciones cibernéticas en un conflicto armado"[27]. Esta opinión, como se puede comprender, requiere la definición previa que declare un ciberataque como acto de guerra (*jus ad bellum*).

23 Martin C. Libicki, *Cyberdeterrence*, Prepared for the United States Air Force Approved for public release; distribution unlimited, Library of Congress Cataloging-in-Publication Data, 2009 https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG8

24 Ibíd.

25 Ibíd.

26 Ibíd.

27 Cordula Droege, *No hay lagunas jurídicas en el Ciberespacio*, Comité Internacional de la Cruz Roja, 16 de agosto de 2011, acceso en internet el 9 de octubre de 2017, en https://www.icrc.org

Para la asesora legal del CICR, el concepto de la guerra cibernética es un tanto impreciso y, al parecer, su significado varía según quién lo use. En el marco de este debate, a diferencia de las tradicionales operaciones militares cinéticas, la guerra cibernética se refiere a los medios y métodos de guerra que se basan en la tecnología de la información y se usan en el contexto de un conflicto armado en el sentido del derecho internacional humanitario[28]. En ese contexto, las operaciones cibernéticas pueden dar lugar a preocupaciones de índole humanitaria, en particular cuando sus efectos no se limitan a los datos contenidos en el sistema informático o en el ordenador afectado. En efecto, habitualmente se pretende que esas operaciones tengan efectos en el "mundo real". Por ejemplo, al interferir con los sistemas informáticos de apoyo, se pueden manipular los sistemas de tráfico aéreo, los sistemas de oleoductos o las plantas nucleares del enemigo. El potencial efecto humanitario de algunas operaciones cibernéticas es, como se ve, de enorme magnitud. Las operaciones cibernéticas realizadas hasta ahora, por ejemplo, en Estonia, Georgia e Irán, no parecen haber tenido consecuencias graves para la población civil. Sin embargo, al parecer es técnicamente factible interferir con los sistemas de control de los aeropuertos, otros sistemas de transporte, diques o plantas nucleares por medio del ciberespacio[29].

Por consiguiente, no se puede descartar la materialización de escenarios potencialmente catastróficos como la colisión de aeronaves, la emisión de sustancias tóxicas desde plantas químicas, o la perturbación de la infraestructura y los servicios vitales como las redes eléctricas o de abastecimiento de agua. Las principales víctimas de esas operaciones serían, con toda probabilidad, las personas civiles[30].

La inexistencia de un marco normativo aplicable de manera particular a la ciberguerra genera una complejidad representada por las características particulares del tipo de guerra que se libra en el espacio. Como lo recuerda Luke, el solo concepto de arma de guerra utilizado en las normas que regulan el conflicto bélico involucra más bien la idea de instrumentos kinéticos utilizados para atacar o defenderse, cuyos efectos son percibidos por los sentidos y producidos contra objetos corpóreos por medios físicos[31]. En esta materia profundiza: "Desde luego, una bayoneta perforando el pulmón de un soldado de infantería encaja dentro de tal concepto. Asimismo, la inhalación de agentes químicos como el Napalm, producen en el cuerpo de

28 Ibíd.
29 Ibíd.
30 Ibíd.
31 Op. cit., Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 414.

la víctima efectos materiales evidentes. Bombardeos aéreos por saturación, envenenamiento o corte de suministros de agua, destrucción de torres y redes eléctricas son también medios cuya utilización, legítima o ilegítima, encajan dentro de los conceptos de arma y conflicto armado del Derecho de Guerra. Sin embargo [concluye], la irrupción de la electrónica y la informática en el ámbito bélico obliga a efectuar algunas piruetas intelectuales a la hora de someter su utilización o abuso a las normas del Derecho de Guerra[32]".

El problema que se advierte en la perspectiva jurídica es cómo aplicar las normas de dicho marco jurídico a la ciberguerra. En este sentido, Luke afirma que "subsumir normas que fueron creadas para aplicarse a acciones y objetos con existencia corpórea, a una realidad compuesta de cosas inmateriales genera problemas que la interpretación analógica no siempre logra resolver. Las armas informáticas solo consisten en información, en pulsos eléctricos organizados bajo códigos lógicos que expresados en un lenguaje matemático pueden traducirse en órdenes ejecutables por un computador"[33]. Asimismo, agrega que[34]:

> *Estas armas tienen como blanco otros códigos, otros sistemas de información, cosas que aun siendo inmateriales permiten en una creciente medida, el efectivo desempeño de toda una sociedad. Las particularidades de este tipo de armas generan una serie de interrogantes desde el punto de vista jurídico. Por ejemplo, surge la duda sobre si se puede concebir como agresión una acción que no ha implicado el traspaso de fronteras físicas protegidas por la soberanía de un Estado, ni la movilización de tropas, ni la muerte de soldados o civiles en el Estado víctima del ataque, ni la destrucción de bienes físicos como edificios, represas o caminos. Asimismo, es objeto de debate determinar si un ataque informático que logra causar un perjuicio físico o económico de carácter sustancial en el Estado Víctima, justifica o no, desde el punto de vista del Derecho Internacional, una respuesta armada de este o la responsabilidad de aquel.*

En este escenario jurídico de incertidumbre, el CICR entrega una visión que en algo aclara el punto, nuevamente en el ámbito del *jus in bello*. Señala el CICR que si bien el DIH no contenga referencias específicas a las operaciones cibernéticas no significa que esas operaciones no estén sujetas a sus normas. Si los medios y métodos de la guerra cibernética producen los mismos efectos en el mundo real que las armas convencionales (destrucción, desorden, daños, lesiones o muerte), se rigen por las mismas normas que las armas

32 Ibíd.
33 Ibíd.
34 Ibíd.

convencionales[35]. Agrega el CICR que la tecnología evoluciona sin cesar, y el DIH es suficientemente amplio para abarcar todas las nuevas tecnologías. El DIH prohíbe o limita el uso de determinadas armas (por ejemplo, las armas químicas o biológicas, o las minas antipersonal). Pero por medio de sus normas generales regula todos los medios y métodos de guerra, incluido el uso de todas las armas. En particular, el artículo 36 del Protocolo adicional I a los Convenios de Ginebra establece lo siguiente: "Cuando una Alta Parte contratante estudie, desarrolle, adquiera o adopte una nueva arma, o nuevos medios o métodos de guerra, tendrá la obligación de determinar si su empleo, en ciertas condiciones o en todas las circunstancias, estaría prohibido por el presente Protocolo o por cualquier otra norma de derecho internacional aplicable a esa Alta Parte contratante"[36].

Concluye el CICR señalando que más allá de la obligación concreta que impone a los Estados Partes, la norma precedente demuestra que las disposiciones generales del DIH se aplican a las nuevas tecnologías. Esto no excluye la posibilidad de que sea necesario seguir desarrollando esta rama del derecho a medida que evolucionen las tecnologías o que sus consecuencias humanitarias se comprendan mejor. La determinación de esa necesidad incumbe a los Estados. Mientras tanto, es importante destacar que no hay lagunas jurídicas en el ciberespacio. Más allá de esta afirmación, se plantean muchas preguntas acerca de la forma de aplicar el DIH en la práctica[37].

Sin perjuicio de lo señalado por el CICR, lo cierto es que la ciberguerra se encuentra huérfana de un marco normativo más preciso y con mayores certezas. En especial, este marco es requerido por los órganos y cuerpos militares y técnicos que emplean estos medios en el marco de un conflicto armado. Como se puede comprender, a veces en un conflicto armado la línea que marca la diferencia entre lo legal y lo ilegal respecto del uso de medios y métodos puede resultar confuso. Las condiciones del campo de batalla hacen difícil marcar con exactitud cuándo se está dentro o fuera de lo permitido, en particular considerando la aplicación de los principios que orientan el derecho internacional humanitario (distinción, proporcionalidad). De ahí la importancia de contar con reglas claras para el uso de medios y métodos de guerra en ciberguerra.

La falta de respuesta jurídica precisa en ciberguerra, en particular en el campo del *jus in bello*, genera la necesidad avanzar en la identificación de propuestas que, aun cuando en un carácter no vinculante, entreguen caminos que orienten la conducta de los Estados y de las partes combatientes, en

35 Op. cit., Droege, Cordula, *No hay lagunas jurídicas en el Ciberespacio.*
36 Ibíd.
37 Ibíd.

particular las Fuerzas Armadas, al momento de decidir el uso del ciberespacio para fines militares, en el ámbito de un conflicto armado. De esto trata el siguiente apartado.

Hacia el desarrollo de un marco normativo en ciberguerra

Un punto de especial y previa consideración en materia de ciberguerra es que los medios y métodos de ciberguerra no están, en principio, prohibidos. Es decir, la ciberguerra, a diferencia del cibercrimen y el ciberterrorismo, como tal no cae *per se* en el campo de la ilegalidad. En ese contexto, el Derecho está llamado a establecer un conjunto de normas que regulen y precisen el uso de los medios y métodos de ciberguerra, en orden a prohibir o restringir su empleo, y por esta vía evitar que su uso genere consecuencias que resulten desproporcionadas o dañen a personas y recursos que no están relacionadas con el ámbito militar o bélico del conflicto[38].

Señalado lo anterior, es posible comentar que el trabajo ya citado de Luke presenta un marco de análisis que resulta útil para comprender las dificultades que reviste construir un modelo de derecho que aplique con eficiencia en la regulación de la ciberguerra[39]. A modo de síntesis, y luego de descartar propuestas que la doctrina internacional plantea respecto de normas vigentes que podrían servir como marco jurídico en la materia[40], este marco de análisis se construye de las siguientes variables o premisas.

- Mientras la regulación en ciberguerra no exista, los Estados deben valerse del Derecho vigente.
- En el Derecho vigente no hay claridad acerca de cómo o por qué podría perseguirse la responsabilidad de los Estados agresores.
- Existen dificultades que sortear para admitir la viabilidad para la aplicación del derecho vigente. Estas dificultades tiene que ver con:

[38] En esta materia, la Regla 12 del Manual de Tallinn, que será citado a continuación, ilustra el punto. Esta regla señala que "Una ciberoperación, o una amenaza de ciberoperación, constituyen una amenaza ilegal de fuerza cuando la acción amenazadora, si es llevada a cabo, sería un uso de fuerza ilegal".

[39] Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* pp. 415-421.

[40] Estas doctrinas son 4: 1) sobre tratados de no proliferación nuclear, 2) sobre tratado antártico y derecho del Espacio; 3)Convención de las Naciones Unidas sobre Derecho de los Tratados del Mar, 4) sobre asuntos de Asistencia Legal. En Op. cit. Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* pp. 416-417.

  - Establecer si frente a un ataque informático se está bajo las normas del *jus ad bellum* o bajo las normas del *jus in bello.*
  - Establecer si un ciberataque logra calificar como un uso de la fuerza prohibido; esto debido al tipo de arma que se emplea en este tipo de ataque, diferente al carácter kinético que tienen las de guerra convencional.
- Respecto de la calificación de uso de la fuerza prohibido, existen dos escuelas. La primera es la que resta importancia a los medios con que se lleva a cabo el ataque y se concentra en los daños provocados; la segunda, que cualquier cosa distinta a un ataque armado no está prohibida por el derecho Internacional.
- La propuesta en orden a adecuar el Derecho Internacional vigente a la ciberguerra conduce a dos soluciones distintas. La primera es homologar los ciberataques a ataques armados convencionales. La segunda, reconstruir estas agresiones hacia conductas típicas de la ley penal del país víctima.

Hacia la construcción de un marco normativo. El Manual de Tallinn

El curso de acción hasta ahora elegido para cubrir el vacío regulatorio existente en materia de ciberguerra es la homologación del Derecho vigente a este ámbito. En efecto, y como lo propone el CICR, no existiendo desarrollo normativo especial y vinculante en ciberguerra, lo que se formula es aplicar el actual marco regulatorio del derecho internacional de los conflictos armados. En particular la Carta de la Organización de Naciones Unidas en lo referente a la legalidad en la decisión de uso de la fuerza, *jus ad bellum*, y las reglas del derecho internacional que regulan, con arreglo al derecho humanitario, *jus in bello,* el uso de la fuerza durante el conflicto para evitar daños innecesarios a los propios combatientes, a la población civil y sus bienes.

Para lo anterior, se ha avanzado en el desarrollo doctrinario desde el campo académico, proponiendo un conjunto de reglas que, derivadas del marco jurídico vigente, permiten su aplicación a la ciberguerra. El trabajo más relevante es el proyecto llevado a cabo por 20 renombrados académicos, los que, por una invitación del Centro de Excelencia Cooperativo en CiberDefensa, de la Organización del Tratado del Atlántico Norte (NATO, por sus siglas en inglés), durante tres años estudiaron el derecho internacional aplicable a la ciberguerra. Este trabajo dio vida en el 2013 al llamado "Manual de Tallinn" –en adelante "el Manual"–, el que propone 95 reglas no vinculantes que regulan el ejercicio de este tipo de guerra en el

ciberespacio[41]. Como señala el Manual en su parte introductoria, su texto se enfoca a tópicos de soberanía, responsabilidad de los Estados, unido a los ya señalados *jus ad bellum y jus in bello,* para finalizar con las leyes de la neutralidad. Para cada uno de estos ámbitos el Manual explicita reglas particulares, acompañada de comentarios que las relacionan con normas del derecho convencional y consuetudinario. Estos comentarios explican además cómo el grupo de expertos convocados interpretó las normas existentes al contexto cibernético, incluyendo por último en estos comentarios los desacuerdos en el trabajo de interpretación[42].

El Manual de Tallinn, texto de cuidadosa elaboración, y que sugiere un marco regulatorio, no vinculante, para su aplicación en el marco del conflicto, abarca una categoría de materias diversas, las que van desde la responsabilidad de los Estados, reglas para el uso de la fuerza, reglas de conducción de hostilidades, hasta materias acerca de neutralidad de los Estados y relativos a ocupación. Respecto de esta propuesta, interesa de manera particular señalar lo siguiente de acuerdo con los criterios y reglas del Manual.

- Atribuye la responsabilidad del Estado cuando personas o ciberestructuras de su jurisdicción realizan actos contrarios al Derecho Internacional.
- Determina el hecho del uso de la fuerza de medios y métodos cibernéticos como constitutivo de conflicto armado cuando estos llegan al nivel o intensidad de uso de la fuerza de medios convencionales, calificado así por el derecho internacional. Es por tanto una metodología de homologación de unos respecto de otros. El indicador para medir esta intensidad está dado fundamentalmente por el nivel de daño causado (escala y efectos de la operación cibernética).
- El derecho a defensa de un Estado ante ataques cibernéticos, como la decisión de uso de la fuerza del Consejo de Seguridad de Naciones Unidas, puede incluir tanto medidas de fuerza convencionales como cibernéticas.
- La existencia de un conflicto armado, internacional, o sin el carácter de internacional, puede verificarse ante el solo uso de medios y métodos cibernéticos, no requiriéndose necesariamente el uso de otros medios convencionales para calificarlos como tales.

41 *Tallinn Manual on the International Law Applicable to Cyber Warfare*, London, Cambridge , Cambridge University Press, 2013.

42 El 2017 se publicó el Manual de Tallinn 2.0, de Derecho Internacional aplicable a ciberoperaciones. Esta versión, preparada durante 4 años a partir del 2013, abarcó además aspectos del derecho internacional en ciberguerra en regímenes legales de tiempo de paz. Para el presente estudio, esta versión 2.0 del Manual se toma solo a modo referencial, toda vez que no modifica de manera sustancial las materias que son tratadas en la versión del 2013.

- Define como sujetos de ciberataques a la categoría de personas que el derecho internacional humanitario entiende y define como personas que participan del conflicto. Al mismo tiempo establece como personas protegidas de ciberataques a las que este mismo derecho internacional humanitario protege.
- Identifica los medios de ciberguerra como ciberarmas y sus cibersistemas asociados y métodos de ciberguerra como cibertácticas, cibertécnicas y procedimientos por los que son conducidas las hostilidades.
- Identifica de manera particular como objetivos militares los computadores, redes de computación e infraestructura cibernéticas, tanto de uso militar permanente como aquellos que presentan uso dual, o de uso generalmente civil pero que de manera transitoria se les asigna uso militar. Incluye también la *data* contenida en estos sistemas.
- Aplica de manera homóloga a la ciberguerra las normas de derecho internacional humanitario referidos a conductas y precauciones en el ataque.

En esta revisión de criterios y reglas que establece el Manual, interesa comentar de manera particular la Nº 22. Esta califica como conflicto armado el hecho de que un Estado realice sobre otros ciberataques, sin necesariamente el uso de otros medios y métodos de guerra. Se estima que esta calificación abre un espacio discrecional mayor para que el Estado "agredido" por el ciberataque, sin empleo de otras armas, califique este ataque como constituyente de conflicto armado y, en consecuencia, se arrogue el derecho de responder al amparo de legítima defensa, o al Consejo de Seguridad de actuar en tal sentido, no solo con medios y métodos cibernéticos, sino también en virtud de lo establecido en la regla Nº 14, con medios convencionales. Esta regla, constituiría por tanto una ampliación en la aplicación del principio de la legítima defensa.

Comentarios finales

Estos comentarios pretenden destacar aquellos aspectos que resultan relevantes de la relación existente entre la ciberguerra y el Derecho.

Un primer punto a comentar es constatar la pertenencia de la ciberguerra a un género mayor y que, junto con esta, albergar otras formas de uso del ciberespacio con el fin de generar efectos dañosos en un adversario, o bien efectos lucrativos prohibidos. La ciberseguridad está llamada a evitar los

daños que produce el cibercrimen, el ciberterrorismo y la ciberguerra. Esta última, dependiendo de la doctrina de los respectivos Estados, comprendida a su vez en el marco de la ciberdefensa.

Teniendo como característica común a todas estas formas el uso del ciberespacio, desde la perspectiva del Derecho existe una diferencia fundamental de la ciberguerra respecto de las otras. Esta radica en el hecho de que el uso del ciberespacio en el contexto de un conflicto armado, para fines de conseguir los objetivos e intereses de las partes, no está por regla general prohibido. Más bien, y ya que los medios y métodos cibernéticos son asimilados al concepto de armas destinadas a producir daño en el adversario, la decisión de empleo (*jus ad bellum*) y la forma de empleo (*jus in bello*) están llamados a ser regulados, pero no prohibidos, por el Derecho. Esta regulación debiese estar orientada, primero, a establecer las condiciones de legalidad en la decisión del uso de estos medios y métodos; segundo, a definir formalmente el carácter jurídico de los mismos, definiéndolos, como se ha visto en este trabajo, de una manera similar al resto de las armas que se emplean en un conflicto; por último, a precisar respecto de la forma legal de uso de estos medios y métodos cibernéticos en el marco del conflicto.

Un segundo aspecto a constatar es la inexistencia de un marco jurídico regulatorio vinculante a nivel internacional, al menos en materias no cubiertas por las normas concernientes a cibercrimen. Esta carencia tiene, como se comprenderá, efectos directos en el campo de la ciberguerra. No obstante esta realidad, a nivel regional se aprecian los esfuerzos para generar políticas y reglas en materia de ciberseguridad y ciberdefensa, entre estas, las que se tratan en el marco de UNASUR, esfuerzos que todavía se encuentran en un estado incipiente. También destaca la visión del CICR, en la que propone la aplicación del Derecho Internacional Humanitario vigente a la ciberguerra. Por último, a nivel nacional, la dictación de la Política Nacional de Ciberseguridad y el mandato a desarrollar una política en ciberdefensa, permite albergar la posibilidad de avanzar en aspectos regulatorios más concretos.

Lo anterior, sin embargo, no resuelve el aspecto preciso de la ciberguerra. Como fue señalado, el ámbito específico en que esta se da, la guerra o el conflicto armado, no está prohibido, sino circunscrito a condiciones especiales para decidir su uso y para regular el empleo de medios y métodos una vez iniciado. La ausencia de normas en la materia, como ha sido advertido en este trabajo, ha abierto el campo a discurrir diversas formas de solución en el ámbito internacional. En definitiva, la que ha prevalecido es la de homologar las normas generales respecto de la autorización de uso de la fuerza establecidas en la Carta de Naciones Unidas y del derecho de guerra en convenciones y tratados acerca de derecho internacional humanitario, a

los medios y métodos de ciberguerra. En este sentido, se puede afirmar que esta forma de solución incorpora a la ciberguerra como una forma especial de uso de fuerza en el marco de un conflicto armado.

El poner atención a un marco normativo en materia de ciberguerra, aun cuando sea difícil de distinguir, es algo a considerar para un país como Chile. En este sentido, señala Luke que "Para aquellos Estados cuyas fortalezas no se basan en su arsenal bélico ni en su poder económico sino en su prestigio, el respeto del Derecho Internacional es un factor de suma relevancia. Por ello, el costo de llevar a cabo acciones u omisiones que puedan considerarse como un uso ilegal de la fuerza (o tan solo una ilegítima amenaza de su uso), puede ser sumamente alto en términos de prestigio internacional"[43]. Concluye que "Frente a este hecho y considerando que Chile mantiene una política exterior que otorga alta importancia al prestigio, un conocimiento acabado del marco jurídico internacional que lo protege y obliga frente a las amenazas a la seguridad propias del siglo XXI, es esencial"[44].

En consideración a lo anterior, es pertinente destacar al actual valor de uso del Manual de Tallinn. Si bien sus reglas no generan obligaciones a los Estados por su carácter no vinculante, lo que incluye a Chile, una lectura y análisis preliminar de sus contenidos lleva a afirmar que estas no son contrarias ni al actual Derecho Internacional (*jus ad bellum* y *jus in bello*) ni al propio Derecho Nacional. Por lo mismo, de confirmarse lo anterior con un estudio más acabado, sería pertinente evaluar la posibilidad de incorporarlas a las respectivas doctrinas operacionales de las Fuerzas Armadas de los Estados, en particular de Chile. Esta propuesta, en particular, no se distancia del Derecho Internacional Humanitario de carácter convencional, toda vez que este constituye un marco o estándar de exigencia mínimo que se exige a los Estados. A partir de este mínimo, los Estados pueden adoptar disposiciones que restrinjan más aún el empleo de medios y métodos, entre estos lo de naturaleza cibernética. Constituye por tanto una materia que podría someterse a consideración de las respectivas unidades de doctrina de las ramas castrenses.

43 Op. cit., Victor Luke, *Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas,* p. 415.

44 Ibíd.

Bibliografía

Textos

Candela Justribó, *Ciberdefensa: Una visión desde la UNASUR,* ensayo presentado en el VII Congreso del Instituto de Relaciones Internacionales, La Plata, Argentina, 26.27 y 28 de noviembre de 2014.

Gobierno de Chile, *Política Nacional de Ciberseguridad 2017-2022.*

Gaitán Rodríguez, Andrés *El Ciberespacio: un nuevo teatro de batalla para los conflictos armados del siglo XXI,* Bogotá, Escuela Superior de Guerra de Colombia, 2012.

Luke, V. (2012). Seguridad Informática y Derecho Internacional Público en el siglo XXI: desafíos jurídicos frente a la protección de infraestructuras informáticas. *Revista de Derecho Público.*

Reguera Sánchez, Jesús, *Aspectos Legales en el Ciberespacio. La Ciberguerra y el Derecho Internacional Humanitario,* Grupo de Estudios en Seguridad Internacional, GESI, Universidad de Granada.

Tallinn Manual on the International Law Applicable to Cyber Warfare, London, Cambridge, Cambridge University Press, 2013.

Internet

Carilini Agnese, *ISIS: Una nueva amenaza en la era digital,* Madrid, Instituto Español de Estudios Estratégicos (i.e.e.e.es), 129/2015, (Documento en línea, 1 de diciembre de 2015), en internet http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO129-, [Fecha de consulta el 05 de diciembre de 2017].

En Gobierno de Chile, *Una Política Nacional de Ciberseguridad para Chile,* en internet, http://www.ciberseguridad.gob.cl/noticias/una-politica-nacional-de-ciberseguridad-para-chile/, [Fecha de consulta, el 14 de septiembre de 2017].

Naciones Unidas, Asamblea General, septuagésimo segundo período ordinario de sesiones de la Asamblea General, en Internet http://www.un.org/es/ga/72/agenda/index.shtml, [Fecha de consulta, el 25 de septiembre de 2017].

UNASUR, VII Reunión Ordinaria del Consejo de Jefas y Jefes de Estado, Declaración de Paramaribo, numeral 29.

UNASUR, Consejo de Defensa Suramericano, Acta 1° Reunión Virtual Grupo de trabajo Ciberdefensa CDS-UNASUR, (Documento en línea 7 de marzo de 2017).

Gobierno de Chile, depósito de instrumento de adhesión. En internet http://www.minrel.gov.cl/chile-deposita-el-instrumento-de-adhesion-al-convenio-de-budapest-sobre/minrel/2017-04-21/175923.html, [Fecha de consulta el 16 de diciembre de 2017].

Capítulo 7

Desafíos para afrontar la ciberguerra

Equipo CEEAG

Hacia los alcances de la resiliencia de un cibersistema

A nivel regional[1], los países que han destacado por ser víctimas de un gran número de ciberataques en Latinoamérica fueron Brasil, Argentina, Colombia, México y Chile. Los accesos o robo de información desde un ordenador infectado –denominados *botnets*– predominaron en la región. Incluso, un tipo específico de este código malicioso llamado *dorkbot* generó más de 80 mil acciones contra el sistema virtual, concentrándose en Chile (44%), Perú (15%) y Argentina (11%). Con ello evidenciamos que hace bastante tiempo que el ciberespacio dejó de ser parte de la ciencia ficción para convertirse en uno de los principales espacios de interacción social[2].

El concepto de resiliencia es definido por Holling como "las condiciones de un sistema complejo alejado del equilibrio, donde las inestabilidades pueden transformar al mismo para que presente otro régimen de comportamiento, así la resiliencia es medida por la magnitud de perturbaciones que pueden ser absorbidas por el sistema antes de que sea reorganizado con diferentes variables y procesos"[3]. Entonces, el concepto de la resiliencia está directamente asociado con la sustentabilidad de todo sistema complejo.

1 P. Prandini y M. Maggiore, M. 2013. *Ciberdelito en América Latina y el Caribe.* Una visión desde la sociedad civil. Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y el Caribe, p. 3.

2 Marcos Robledo Hoecker, Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad, PNCS 2017, p. 9.

3 Arturo M Calvente, *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales.

La resiliencia no es una propiedad absoluta y fija sino que, por el contrario, es variable en el tiempo y el espacio y depende, en gran medida, de las acciones y relaciones del sistema y la volatilidad ambiental del contexto en el que se encuentre.

Entonces, si por motivos antes mencionados un sistema comienza a "perder" resiliencia, se incrementa el "potencial de cambio", es decir, aumentan las posibilidades de pasar a un estado o configuración organizacional diferente, incluso si está sujeto a perturbaciones pequeñas o perturbaciones que anteriormente eran insignificantes o no producían ningún efecto adverso.

Al hablar de un sistema robusto, ello debe ser entendido como la magnitud de volatilidad que puede ser compensada por el sistema complejo antes de llegar al colapso de sus características, procesos y funciones principales. Para ello, el diseño debería contemplar dentro del sistema un arquetipo de detección, otro de protección, uno compensatorio, y por último uno de desafío o contraagresión (eventual). Cada uno juega un rol en el proceso y no necesariamente son secuenciales en su actuar, sino que pueden operar en forma simultánea, cooperativa y coordinada. Así el modelo de detección estará monitoreando constantemente la red, para una vez detectada una amenaza real o potencial, activar las alertas o alarmas.

Acá inicia su labor el modelo de protección, con las contramedidas que estén asociados al tipo de evento malicioso captado, las que pueden contener acciones automatizadas como también otras que el controlador aplique a criterio, dando así dinamismo a la respuesta.

El modelo compensatorio operará sobre la base de los recursos de redundancia y robustez del sistema, logrando con ello un grado abordable de resiliencia.

A lo anterior podría sumarse el modelo de desafío, que junto con tener una capacidad exploratoria (control de daños) y otra ciberforense, van en busca de la fuente de la agresión y aplican medidas de bloqueo, neutralización o mitigación de la acción hostil.

El concepto CSIRT

Una de las herramientas más usadas y de respuesta más oportuna ante eventos cibernéticos corresponde al CSIRT. La sigla CSIRT proviene de la expresión en idioma inglés Computer Security Incident Response Team, que traducido al español es Equipo de Respuesta ante Incidencias de Seguridad. Su practicidad se basa en su capacidad de monitoreo constante de las redes, disponiendo de herramientas tecnológicas y personal especializado que

pueden detectar anomalías en el sistema, pero principalmente en disponer de medios de defensa para el bloqueo, reparación o mitigación del efecto de ataques o alteraciones.

Para garantizar la efectividad de un CSIRT[4], la confianza es un requisito muy importante, y la única manera de desarrollar esta condición mediante un historial de colaboración y participación en la comunidad de seguridad. Tiene una importancia menor que el CSIRT sea operado por el gobierno, un proveedor de red, una entidad comercial o la academia, siempre y cuando se desarrolle en asociación con toda la comunidad de trabajo en red y seguridad dentro de la región.

No puede subestimarse la necesidad de contar con CSIRT robustos en empresas, la academia y el gobierno. Los gobiernos tienen un importante papel que desempeñar en motivar el desarrollo de estos equipos, así como percatarse que no pueden "imponer" la confianza que les permita alcanzar sus metas: deben identificar quién les otorga seguridad, fomentar su crecimiento para el país en general y trabajar con todos. La confianza también está ligada a los servicios que un CSIRT ofrece. Cuando un CSIRT se centra correctamente en responder y mitigar un incidente, a menudo las corporaciones y organizaciones extranjeras confiarán más en ellos y proveerán mayor información para apoyar su misión.

Esta información puede limitarse cuando el CSIRT cumple un papel en la persecución criminal o es parte de un servicio de inteligencia. El tipo de información proporcionada a cualquiera de estas organizaciones tiende a ser diferente y los roles, por tanto, deben segregarse debidamente.

Cuando existe una red de CSIRT, es importante la creación continua de su capacidad. Vemos tres niveles diferentes de mejoramiento en la prestación de servicios de los CSIRT:

Competencia

Una competencia define una actividad medible que puede ser desempeñada como parte de las funciones y responsabilidades de una organización. Para el propósito del marco de servicios de los CSIRT, las competencias pueden definirse como los servicios más amplios o como tareas, subtareas o funciones necesarias.

[4] Observatorio de la Ciberseguridad en América Latina y el Caribe, *Ciberseguridad, ¿Estamos preparados en América Latina y el Caribe?*, Informe Ciberseguridad 2016, presentado por OEA y BID.

Capacidad

La capacidad define el número de ocurrencias simultáneas de una competencia en particular que una organización puede ejecutar antes de alcanzar alguna forma de agotamiento de recursos.

Madurez

¿Qué tan bien puede usted hacerlo? La madurez define el grado de eficacia con el que una organización ejecuta una competencia, en particular dentro de la misión y las autoridades de la organización.

Es necesario centrarse en cada uno de estos tres elementos con el fin de tener éxito en el aumento de la eficacia de un programa de CSIRT.

Como tal, es importante para la comunidad de respuesta a incidentes reconocer estas diferencias y trabajar respecto de las maneras de abordarlas, lo que podrían hacer siguiendo estos (o algunos) lineamientos[5].

- Los Equipos de Respuesta a Incidentes que actúen en primera instancia pueden hacer contacto con otros para mitigar ataques.
- Los CSIRT, al trabajar coordinados y en equipo frente a un incidente, deben tender a hablar el mismo idioma operativo y contar con procedimientos claros y expectativas precisas acerca de. uso de la información proporcionada.
- La comunidad CSIRT debe estar dotada de herramientas y técnicas que permitan el intercambio automatizado de información.

Los analistas aprovechan la información para comprender verdaderamente las ramificaciones del incidente y toman las decisiones acertadas para reducir los riesgos mientras mitigan el ataque. Para llegar a este punto, vemos necesario el desarrollo de una red de CSIRT sólida e incluyente, la disponibilidad de formación y educación para los miembros de la comunidad y la necesidad de contar con prácticas estandarizadas dentro de esta estructura de colaboración.

Idealmente la comunidad de CSIRT debería lograr que cada organización cuente con una capacidad de respuesta a incidentes bien equipada. Puede ser un solo individuo o un equipo pequeño, pero cada organización debe poder asumir la responsabilidad por el tráfico que genera. Sin embargo a causa del gran número de redes y su respectivo crecimiento, esto podría considerase

5 Op. cit., *Observatorio de la Ciberseguridad*, OEA y BID.

un panorama complejo de lograr. Una alternativa es que cada país desarrolle su "CSIRT de último recurso", es decir, que puede ser punto de coordinación para aquellas redes que puedan no tener un equipo de respuesta a incidentes bien entrenado y directamente accesible. Se debe entender que, al final, cada organización es responsable de su propia seguridad; un equipo nacional solo puede apoyar en la coordinación pero no podrá "desconectar" o investigar cada máquina comprometida.

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[6], son todos factores en que el ariete ofensivo de la ciberdefensa ciertamente va a aportar.

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[7].

A mejor entendimiento de la amplitud del escenario a cubrir[8], un esbozo de 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 del Reino Unido del 2010[9]. 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

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

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

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

9 Ministerio de Defensa del Reino Unido, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Reino Unido.

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 se ha planteado que la ciberdefensa requiere ser considerada como un nuevo eje estratégico.

La respuesta para ello contemplada en el *Libro Blanco de la Defensa de Francia 2013*[10] plantea un concepto en extremo interesante y que encaja plenamente 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.
- El desarrollo de herramientas especializadas (laboratorios técnico-operativos, redes de ataque, etc.).
- La formulación de una doctrina de empleo de las capacidades de LIO (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.

En el contexto regional[11] 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.

10 Ministerio de Defensa de Francia, *Le Livre Blanc sur la Défense et la Sécurité Nationale*, Ed. 2013.

11 CEEAG, *Observatorio,* Informe Mensual, Ciberdefensa-Situación a la fecha, septiembre 2016.

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 en cada uno de ellos, donde los requerimientos operacionales han tenido una mirada integral y multidisciplinaria, con atención puesta en las nuevas tecnologías, capacitación y preparación de personal técnico, como también la participación necesaria en conjunto del 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 concerniente a esta temática, bajo la responsabilidad directa o asociada de Chile, Ecuador, Perú, Argentina, Bolivia, Brasil y Uruguay.

Intercambio de información de ciberamenazas

En un mundo en el que las tecnologías evolucionan constantemente y los perímetros definidos y las zonas de confianza van desapareciendo poco a poco, los modelos tradicionales de seguridad están sometidos a una presión sin precedentes. Para ser eficaces, los modelos de seguridad deben adaptarse a la nueva realidad.

Ya existe una gran variedad de modelos para compartir inteligencia respecto de amenazas, y algunos llevan aplicándose más de 20 años[12]. Otros están evolucionando para adaptarse a los cambios en el panorama de las amenazas, y los hay que se encuentran en su fase inicial, mientras las fuerzas de seguridad, los proveedores de servicios de seguridad, el sector público y las empresas objetivo exploran métodos que permitan compartir la información y responder de manera eficaz a las modificaciones del marco normativo.

El intercambio de información acerca de amenazas ha sido un proceso lento y manual. Las empresas se han mostrado por lo general reticentes a compartir ni siquiera los más mínimos detalles de los ataques o los sistemas comprometidos, bien por miedo a demandas judiciales o al daño a su reputación, o simplemente para evitar divulgar vulnerabilidades no corregidas.

12 *Informe de McAfee Labs sobre amenazas*, abril de 2017.

Pese a ello, ha habido avances concretos en la conformación de los Centros ISAC, las ISAO y los CERT o CSIRT.

Los centros ISAC (Information Sharing and Analysis Centers) son organizaciones sin ánimo de lucro que actúan como puntos centralizados de intercambio y recopilación de inteligencia relativas a amenazas entre las agencias locales y nacionales, sectores verticales específicos y distintas infraestructuras críticas. Muchos de ellos comenzaron como resultado de una directiva presidencial de EE.UU. de 1998 destinada a promover el intercambio de inteligencia relacionada con amenazas y vulnerabilidades entre propietarios y operadores de infraestructuras críticas. Aunque en un primer momento se centraban en las infraestructuras estadounidenses, muchos centros ISAC han ampliado su cobertura para incluir miembros de todo el mundo. Se han creado igualmente centros ISAC también en sectores distintos de las infraestructuras críticas, como por ejemplo, los del automóvil, aviación, electricidad, comercio, servicios financieros, energía nuclear y abastecimiento de agua, entre otros.

Las organizaciones ISAO (Information Sharing and Analysis Organizations) tienen un campo de acción más amplio que los centros ISAC y constituyen un mecanismo suplementario para promover y apoyar el intercambio de información de amenazas. Su creación fue promovida por una ley estadounidense aprobada en 2015 cuyo objeto era limitar las responsabilidades legales por el intercambio de información pertinente a amenazas con otras empresas. Estas organizaciones pueden también ser privadas o sin ánimo de lucro, especializadas por tipo de amenaza o zona geográfica, y van de comunidades de interés a agencias gubernamentales, pasando por empresas de servicios.

Aplicación de la ciberguerra en un campo de batalla moderno

La ciberguerra puede aparentar ser una amenaza menor, pero se debe considerar que, a diferencia de la guerra convencional, para el desarrollo de sus acciones puede optarse por opciones que requieren reducidos recursos. Basta con contar con los conocimientos y menos de US$10.000 en equipos para convertirse en un "guerrero de la información"[13]. Es más, en un nivel básico de ciberguerra, el solo arriendo de una estación de trabajo en un

[13] Gregory Walters, *A new way of war in the information age*, Univesity of Otawa, Otawa, 1998, p. 3.

cibercafé, a un precio ínfimo, bastaría para generar un daño no menor en una red informática abierta a Internet, si se cuenta con los conocimientos para ello.

En respuesta a lo anterior, las organizaciones tienden a aumentar los recursos asignados para dar mayor seguridad a sus sistemas informáticos, pero la experiencia indica que los riesgos no desaparecen, sino que por el contrario, día a día se develan nuevas amenazas o debilidades que vienen a aumentar los incidentes, de origen interno y externo, existiendo una variedad de razones para ello, dentro de estos figuran[14]: el grado de conectividad se incrementa a niveles que sobrepasan la capacidad de control; la necesidad operacional de integrar elementos de *hardware* y *software* de mayor tecnología, lo antes posible y a menor costo, reducen la introducción de elementos de seguridad, o contramedidas que impiden que sean probados adecuadamente; la aplicación de medidas de seguridad nuevos a sistemas ya existentes es de alto costo y en algunos casos imposible, con serio impacto en su funcionamiento operativo.

Es conveniente señalar que todas las redes y sistemas informáticos, sin importar sus capacidades y cualidades, resguardos u otros, en alguna medida son vulnerables a la ciberguerra, por tanto, factibles de penetrar, destruir, modificar, etc., en función del factor tiempo, recursos y tecnología.

Por lo anterior, lo importante no es sencillamente lograr contar con una capacidad técnica que permita la aplicación o ejecución de acciones de ciberguerra, sino que se debe considerar una planificación que oriente la ejecución de acciones de ciberguerra al logro de determinados efectos, representados por la consecución de objetivos que permitan su materialización.

Se debe tener determinado previamente el momento de ejecución requerido, para así lograr el efecto con la debida oportunidad, previendo los tiempos necesarios para que ello ocurra.

La ciberguerra no obtiene efectos por sí sola, sino que debe asociarse al empleo de todos los recursos disponibles que permitan asegurar su éxito.

La aplicación de la ciberguerra en el campo de batalla moderno tiende a dos ejes bases, que son el asociado al proceso de manipulación del enemigo y sus capacidades para tomar decisiones, y por otra parte a la generación de una propia capacidad para obtención de inteligencia.

Para influir en las capacidades para tomar decisiones, la ciberguerra no puede actuar como compartimiento estanco y debe ser coordinada en sus

14 Anderson, Kent, *Intelligence-Based Threat Assesment for Information Networks and Infraestructures*, Global Tech Reserach Inc., marzo 1998, p. 2.

efectos, momento de aplicación y objetivos buscados por el C2 (combate por el Mando y Control), por tanto se deberá tender al empleo de dos o más de estos elementos, para así lograr un efecto de sinergia, lo que catalizará, potenciará, magnificará y asegurará el resultado.

Luego, su ejecución deberá ser enmarcada en una planificación que coordine adecuadamente la ejecución de operaciones psicológicas, operaciones de diversión (o demostración), operaciones de contrainteligencia, destrucción física y guerra electrónica[15].

Con esto se buscará afectar la capacidad de decisión del adversario, lo que en cuanto a ciberguerra puede orientarse a interferir su capacidad de obtención de información útil, degradar sus procesos de gestación de resoluciones y neutralizar sus medios de comunicación y enlace que le permitan direccionar el esfuerzo de búsqueda, tanto como usar o difundir la inteligencia obtenida.

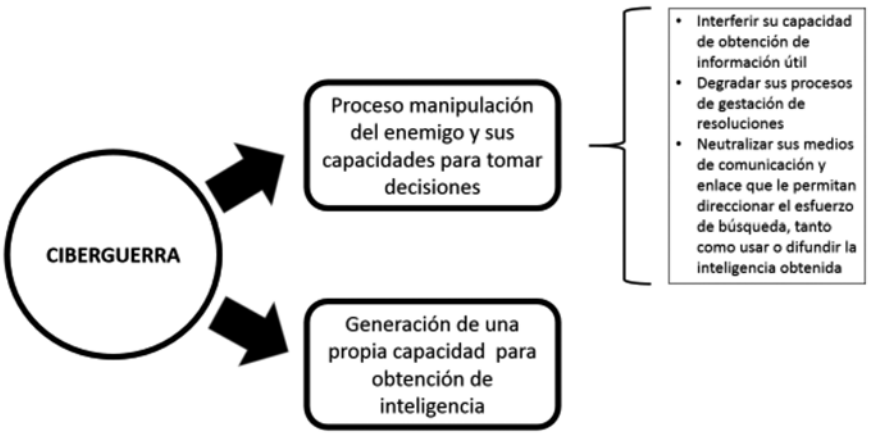
Luego, este proceso de manipulación del enemigo y sus capacidades para tomar decisiones mediante el empleo de la ciberguerra, como uno de sus elementos, podrá actuar en busca de los siguientes objetivos que son propios de lograr mediante la guerra de la información[16]:

- Seguridad informática: afectando la protección a la información y los sistemas informáticos, sus previsiones para el respaldo, restauración, detección y capacidad de reacción.
- Entorno informático: saturando, perturbando, degradando o interrumpiendo la interacción de individuos, organizaciones o sistemas de búsqueda, proceso o difusión de información.
- Superioridad informática: por medio de la negación de la capacidad del adversario de obtener, procesar y difundir información mediante un flujo ininterrumpido.
- Sistema informático: incidiendo en la eficacia de su infraestructura, organización, personal y componentes para degradar o neutralizar su capacidad de obtención, proceso, archivo, transmisión, proyección, difusión y acción.

15 Op. cit., Department of Defense, Ed. Feb. 2000, pág. A48 (Appendix A).

16 Departamento de Defensa de Estados Unidos, *DOD Directive S-3600.1, "Information Operations (IO)".*

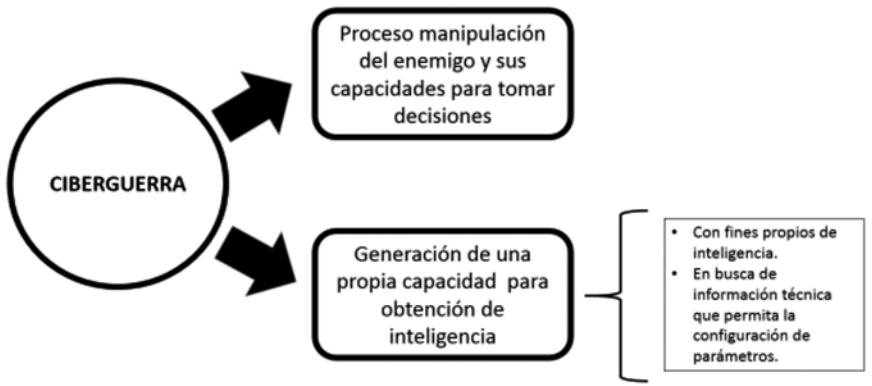
Figura 1
Ejes a los que tiende la aplicación de la ciberguerra



Fuente: Elaboración propia.

La ciberguerra puede ser empleada para la obtención de información con fines propios de inteligencia o en busca de información técnica que permita la configuración de parámetros para la ejecución de otras acciones de ciberguerra.

Figura 2
Ejes a los que tiende la aplicación de la ciberguerra



Fuente: Elaboración propia.

Para ello deberá orientar su acción bajo las normas que son propias de operaciones especiales, es decir, como una suma de acciones ocultas, que emplean para ello técnicas encubiertas, realizadas con medios especializados sobre un objetivo de inteligencia, dentro o fuera del territorio, en tiempo de paz o de guerra y cuyo logro no delata a quienes las inspiran, evitándose así los comprometimientos.

Al actuar en busca de información técnica que permita la configuración de parámetros para la ejecución de otras acciones de ciberguerra, tanto de obtención de información como de generar entrabamiento técnico de las redes objetivo, orientará su acción al logro de información referida principalmente a lo siguiente[17]:

En cuanto a aspectos cuantitativos

- Cantidad e identificación de los administradores de la red: verificar sus horarios de control y acciones rutinarias que permitan detectar vulnerabilidades.
- Número de alarmas activadas: con el fin de poder determinar la cantidad de ataques simultáneos que se requerirán.
- Usuarios detectados: para de esa forma suplantar usuarios y eventualmente generar intrusiones.
- Amenazas reconocidas por el sistema: para configurar medios de ataque que no sean reconocidos por los subsistemas de defensa, alerta y reacción.
- Sistemas de monitoreo: verificar los horarios en que la red se encuentra bajo control y bajo qué nivel de libertad de acción.
- Nodos protegidos: para centrar el ataque en aquellos nodos de mayor vulnerabilidad.
- Cantidad de ataques simultáneos que se requerirán: esta información será importante para la determinación de la cantidad de acciones requeridas simultáneamente, con el fin de generar ataques que atraigan respuestas de reacción y defensa del sistema víctima, distrayéndolo del ataque principal.

17 Myron Cramer, *New Methods of Intrusion detection using Control-Loop Measuremente*, Fourth Technology for Information Security Conference , Houston, Texas, mayo 1996, p. 2.

En cuanto a aspectos cualitativos

- Probabilidad de detección del ataque
- Índice de falsas alarmas
- Rango de detección de intrusión

En cuanto a aspectos de tiempo/oportunidad

- Tiempo de detección
- Tiempo de activación de la alarma
- Cantidad de información o *data* archivada
- Oportunidad de empleo de esa información (inmediato, corto, mediano, largo plazo)
- Históricamente, las acciones de ciberguerra se han desarrollado contra un número limitado de sistemas[18]. El motivo de estos ataques varía, pero los métodos y objetivos se limitaban al subsistema del computador como objetivo primario. Actualmente, un significativo cambio es experimentado al respecto, los avances tecnológicos, junto con intenciones que pasan a ser más criminales o delictuales, generan amenazas de ciberguerra para toda la infraestructura informática.

Una síntesis de su comportamiento nos indica que existen ataques a la infraestructura y otros orientados solo al sistema:

Ataques a la infraestructura

Buscan un significativo compromiso del funcionamiento de toda una infraestructura, más que el afectar sus componentes individuales. De ser exitosos, son capaces de mantener un compromiso del funcionamiento de la red en forma temporal.

Implican la ejecución de acciones contra los sistemas de respaldo y recuperación de archivos y elementos. Son difíciles de implementar, sustentar y lograr éxitos. Requieren una definición previa y precisa de sus objetivos, un ataque coordinado contra múltiples sistemas y puntos de control, en tiempo preciso, con el fin de comprometer los sistemas de redundancia o respaldo.

No todos los ataques de ciberguerra llegan a ser conocidos, ya que algunos no son divulgados por quienes han sido sus víctimas y otros nunca llegan a

[18] Op. cit. Kent Anderson, p. 8.

ser detectados. Un caso conocido contra una infraestructura fue el ejecutado por el Chaos Computer Club, en Alemania, en septiembre de 1995, quienes ejecutaron una acción en contra del sistema de comunicaciones francés, como una forma de protestar por las pruebas nucleares que Francia llevaba a cabo en el Pacífico. Este ataque tuvo pequeño o nada de impacto[19] en lo operacional del sistema, pero sí logró repercusión comunicacional.

Otro caso fue el del martes 27 de junio del 2017, donde algo que ya era esperable se hizo realidad. Una oleada de agresiones cibernéticas atacaba varios objetivos multinacionales. El agente agresor nuevamente se presentaba como un *malware* tipo *ransomware* (que genera una suerte de "secuestro virtual" de los archivos al capturarlos en su origen, encriptarlos y solo devolverlos a su normalidad previo pago de un rescate monetario). Esa agresión fue presumiblemente perpetrada mediante un virus denominado "Petrwrap", que corresponde a una variante "Ransomware Petya" usado en ataques anteriores, con una cercana similitud al "Wannacry", de triste memoria en su megabloqueo del 12 de mayo del 2017, en que afectó a más de 150 países, con efectos que no pudieron ser cuantificados en su totalidad.

Ataques a sistemas

Son acciones de ciberguerra orientadas a afectar sistemas individuales o centros de control, los que no generan la detención de la operación de toda la infraestructura u organización. Sin embargo, corresponde a una intrusión en la que se ve comprometida la integridad básica del sistema. Esto puede acarrear la pérdida de la confidencialidad de la información guardada, la integridad de los archivos o *data*, o afectar la disponibilidad de los recursos disponibles.

Ejemplos de este tipo de ataques con resultado exitoso son muy comunes de conocer, como las efectuadas contra la *web* de la VI Cumbre Iberoamerciana que se realizó en Santiago de Chile en 1996, la acción de *hackers* supuestamente brasileños contra la *web* de la Cámara de Diputados (www.cámara.cl) en el 2000, la intrusión a la *web* del Ministerio Secretaría General de Gobierno (www.segegob.cl) en febrero del 2000, entre otras[20].

Luego, el ataque a un sistema, con un objetivo bien determinado y un efecto perseguido que sea determinante, pasa a ser una de las acciones más rentables en la aplicación de ciberguerra. Por ello, es factible enunciar

19 Ibíd.

20 www.emol.cl *"Hackers atacaron la Web de la Cámara"*, http://hechos.com.do/article/88546/hackers-atacan-pagina-camara-diputados/.

características de los tipos de objetivos rentables a la aplicación de ciberguerra, los que al integrar las características de objetivos ya descritas, variarán de acuerdo con el fin perseguido, pudiendo presentar algunos rasgos comunes, pero serán diferenciables en su forma de explotación. Es así como se han determinado las siguientes:

Características comunes

El efecto buscado con el objetivo deberá ser compatible con otras formas de accionar, específicamente de combate por el C2, para así magnificar y asegurar el resultado.

Características de objetivos para manipular al enemigo

- Será fundamental mantener la acción en forma oculta por el máximo de tiempo que se pueda, no generando instancias de alarma o detección que puedan delatar el empleo de ciberguerra, de lo contrario el adversario buscará la reconfirmación de la información que está procesando, para luego alertarlo que está siendo víctima de medidas contra su sistema informático.
- Tenderán a ser compatibles con el desarrollo de acciones de combate por el C2 centradas en la diversión y en la guerra electrónica (decepción).
- Deberán servir a una historia de diversión.
- Su consecución tendrá un efecto de reducida permanencia, por lo que se requerirá planificar adecuadamente el instante y tiempo de ejecución y prever los lapsos necesarios para que se concrete el efecto con oportunidad.
- Parte del supuesto que las actividades reales son ocultadas mediante encubrimiento, para que así no se descubra que la situación que es presentada al adversario es falsa.
- Este tipo de objetivos requiere que se desplieguen medios de inteligencia que permitan detectar si se está causando el efecto deseado.

Para degradar la capacidad del enemigo de tomar decisiones

- Será difícil mantener la acción oculta, pues el adversario detectará, mediante sus procedimientos de control, que su sistema de mando y conducción se está viendo afectado.

- Su empleo puede considerar la saturación, obstaculización, deterioro, daño temporal o permanente de parte de sus sistemas informáticos de apoyo a la toma de decisiones o gestación de la resolución.
- Considerando que la víctima tenderá a contar con sistemas redundantes o respaldo, su efecto no podrá tener una gran permanencia, por lo que se requerirá planificar adecuadamente el instante y tiempo de ejecución y prever los lapsos necesarios para que se concrete el efecto con oportunidad.
- La rentabilidad del objetivo aumentará mientras mayor sea su conectividad a otros subsistemas o componentes y mientras mayor sea la necesidad del sistema de contar con ese punto para derivar informaciones hacia otros elementos informáticos.
- Este tipo de objetivos, al igual que el enunciado anteriormente, requiere que se desplieguen medios de inteligencia que permitan detectar si se está causando el efecto deseado.
- Su valor como objetivo será inversamente proporcional al grado de capacidad del sistema víctima para proceder a su redundancia, respaldo, restauración o reemplazo. Es decir, mientras menor sea la capacidad para reemplazar un componente del sistema, mayor será su valor como objetivo.
- El valor del objetivo aumentará mientras mayores sean las posibilidades de obtener el efecto por múltiples vías para así asegurar el éxito.

Para la obtención de inteligencia

- Aquellos subsistemas o componentes con baja capacidad de respuesta, detección o alarma a las intrusiones, representarán objetivos de alto valor.
- Los objetivos que tengan características de presentar un alto nivel de falsas alarmas requerirán previamente acciones que hagan perder la confianza de los operadores en ellos, para así retardar o anular sus reacciones. Normalmente este tipo de objetivos se emplearán como elementos secundarios que permitan amarrar la atención de quienes monitorean los sistemas, restando atención a la verdadera intrusión.
- La importancia del objetivo será directamente proporcional al acceso que permita a archivos de *data* de gran valor de uso y calidad. A su vez, la calidad de esa información se relacionará a la oportunidad y pertinencia para su empleo.

Bibliografía

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

Anabalón, Juan y Donders, Eric. Revisión de ciberdefensa de infraestructura crítica, Estudios Seguridad y Defensa Nº 3, ANEPE, Chile, 2014.

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.

Anderson, Kent. *Intelligence-Based Threat Assesment for Information Networks and Infraestructures*, Global Tech Reserach Inc., marzo 1998.

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.

Calvente Arturo M. *Resiliencia: un concepto clave para la sustentabilidad*, Universidad Abierta Interamericana, Centro de Altos Estudios Globales.

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).

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.

Departamento de Defensa de Estados Unidos, *DOD Directive S-3600.1, "Information Operations (IO)"*.

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

Koch, Sebastián. "La política de ciberdefensa en Chile", Columna de Opinión, (Documento en línea) 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.

Mc Afee. *Informe de McAfee Labs sobre amenazas*, abril de 2017.

Myron Cramer. *New Methods of Intrusion detection using Control-Loop Measuremente*, Fourth Technology for Information Security Conference , Houston Texas, mayo 1996.

Observatorio, Informe Mensual, CEEAG, Ciberdefensa-Situación a la fecha, septiembre 2016.

Prandini, P. y Maggiore M., M. 2013. *Ciberdelito en América Latina y el Caribe*. Una visión desde la sociedad civil. Proyecto Amparo, Sección de Estudios. LACNIC Registro de Direcciones de Internet para América Latina y el Caribe.

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

Hoecker Marcos Robledo. Subsecretario de Defensa Secretario Ejecutivo, Comité Interministerial sobre Ciberseguridad, PNCS 2017.

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.

Reflexiones finales

Al concretar estas reflexiones finales concernientes a la ciberguerra, se ha tenido a la vista la definición de los impactos, transformaciones, estructuras, adaptabilidades o cambios en la infraestructura crítica nacional, con ideas que sean aporte a una estrategia de disuasión en ciberguerra. De la misma forma se visualizaron vulnerabilidades, riesgos y amenazas de seguridad, como parte del combate por el mando y control. En ello se establecieron aspectos de atención respecto de nuestra infraestructura crítica.

Así entonces, al haber extendido el análisis de la ciberguerra desde su raigambre técnica a su proyección estratégica, teniendo a la vista sus consideraciones jurídicas o de aplicación ética, emerge desde la investigación y queda de manifiesto la concepción que uno de los constituyentes del mando y control que más puede ser influido corresponde a la integridad de la información. Así las acciones buscan, por una parte, afectar el entorno que da coherencia al contenido discursivo, como otro camina hacia bloquear que los segmentos de información sean emitidos o recibidos en su contextura de origen. La manipulación de acciones ejecutables también será un interesante campo de cultivo para ciberoperaciones. La decepción y manipulación se escudarán en el ocultamiento mientras que la perturbación responderá normalmente al ataque masivo, múltiple y abierto. En engañar, manipular o bloquear estará el dilema. Así, la modificación no autorizada de *data* o instrucciones serán parte de la decepción mientras que el actuar contra las funciones del sistema es parte de la manipulación. El bloqueo actuará sobre la disponibilidad, es decir, la capacidad de acceder a determinada *data* cuando ello es necesario.

La ciberguerra, operando mediante ciberoperaciones, en lo militar ha pasado a constituir un instrumento más para su aplicación en el ámbito de

la defensa, dando pasos sólidos para ser considerada, al menos en sus líneas de ciberdefensa y ciberseguridad, como elementos constituyentes de políticas públicas. Requiere en su concepción no solo una vertiente ofensiva, sino que claramente debe contar con una acentuada raigambre en lo defensivo, dando protección a sistemas, procedimientos vitales y las ya definidas infraestructuras críticas.

Para entender los alcances de la ciberguerra, el análisis debió partir por conocer y comprender los efectos que busca la guerra de la información, y dentro de ella el combate por el mando y control. Así contextualizado su ambiente, la infoguerra surgió como el macrosistema que dio forma a las fortalezas, oportunidades, debilidades y amenazas de la infraestructura crítica.

Levantada entonces la capacidad de operar defensiva u ofensivamente en un plano de ciberguerra, al asociarla a sus efectos en lo estratégico, se infiere que el éxito de la disuasión se basa en consolidar una capacidad de convencer a los adversarios que sus intrusiones cibernéticas implicarán un costo demasiado alto para ellos. Pero cuando los objetivos que nos pueden ser batidos son de un alto valor y el agresor no posee mucho que perder, entonces la ecuación costo-beneficio se torna muy favorable para el atacante y le da una condición asimétrica crítica, generando un atractivo índice neto de rentabilidad.

El factor extraterritorial de la ciberguerra impactará en la ubicación y despliegue geográfico de sus actores, los que no necesariamente serán ubicados dentro de las zonas determinadas por el conflicto, sino que podrán operar desde lugares ignotos o encubiertos cibernéticamente, pero siempre buscando efectos en las áreas que en lo bélico puedan ser rentables. El factor de "profundidad estratégica", en su vertiente clásica, está hoy siendo modificado, por lo que la necesidad de crear estrategias de defensa para proteger las infraestructuras críticas es más que fundamental.

La dependencia a plataformas cibernéticas se está tornando cada día más crítica. Así como en su momento el aire vino a aportar con una nueva dimensión al campo de batalla, no es posible concebir un escenario moderno sin considerar y tomar resguardos de lo que significa el quinto dominio, ya definido como el ciberespacio.

Una política pública en este ámbito reúne 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, resultará sustancial 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. Acá, la condición multidisciplinaria del diseño será factor clave y convivirán

actores de diferentes ministerios, como Interior, Defensa, Transportes y Telecomunicaciones, Energía, entre otros. También lo harán quienes puedan generar sus aportes desde lo académico o desde el ámbito privado. Cada uno de ellos será actor del proceso y gestión, con el aporte de su área de conocimiento en particular.

Acá entonces, el concepto de la ciberdefensa es entendido como bien público, que ya en la investigación ha sido presentada como un nuevo Eje Estratégico, además de considerarla como una nueva dimensión, donde se debe potenciar como factor de capacidad estratégica, lo que es coincidente con la tendencia contemporánea del actuar en el ciberespacio.

Así llevada la ciberguerra, el concepto rector de una estrategia de seguridad nacional está orientado a intentar obtener los objetivos nacionales pacíficamente mediante 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 una 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". Es destacable 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.

El ciberespacio es la expresión de un espacio virtual y vital para que exista la transmisión de la información, donde 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 e iré sobre la fuente de origen.

Aclaremos acá que la detección de una ciberagresión solo justificaría el uso de represalias militares convencionales como viables si sus consecuencias son proporcionales al daño causado por el ciberataque y que pueden ser sólida y claramente comprobables. La legitimidad de una respuesta de este tipo quedaría en entredicho si no se percibe una equidad entre el ataque y la respuesta.

La tendencia futura de la ciberguerra va en escalada. Este aporte que entrega la Academia de Guerra, por medio de su Centro de Estudios Estratégicos (CEEAG), ha buscado aportar en la línea de establecer bases de conocimiento,

proyección de estudios y direccionamiento de análisis. La generación de nuevo conocimiento estratégico será muy necesaria, particularmente relacionado con la disuasión y el combate por el mando y control, que son temas que se proyectan con incremento célere, donde la mirada del investigador deberá estar presente con especial atención respecto de 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.

ANDROS IMPRESORES
www.androsimpresores.cl

OT/38893

"Este aporte, desarrollado por un equipo multidisciplinario de investigadores del Centro de Estudios Estratégicos de la Academia de Guerra (CEEAG), se centró en producir una discusión bibliográfica indispensable para responder a las interrogantes que en lo estratégico nos presenta hoy la ciberguerra, la que opera en un ambiente compuesto por las infraestructuras tecnológicas, los componentes lógicos de la información y las interacciones sociales que se verifican en su interior.

Así, logra sostener que la ciberguerra es un concepto de repercusión estratégica, con un escenario, que es el ciberespacio, que debe ser entendido como una quinta dimensión, lo que es coincidente con la tendencia contemporánea del actuar estratégico.

El principal aporte al área de investigación de ciberguerra está en definir los impactos, transformaciones, estructuras, adaptabilidades o cambios en la infraestructura crítica nacional, proponiendo elementos y acciones que aporten a una estrategia de disuasión en ciberguerra, enunciando vulnerabilidades y riesgos de ciberguerra y las subsiguientes amenazas de seguridad, especialmente en lo que comporta el combate por el mando y control.

El texto no se queda solamente en lo técnico-operativo, sino que luego va a la vertiente relacional entre la ciberguerra y su contrastación con la legalidad vigente, nacional e internacional, principalmente en sus relaciones en el ámbito del Derecho Internacional de los Conflictos Armados y la conflictividad cibernética.

Se cierra con un análisis basado en las amenazas de ciberguerra identificadas, exponiendo advertencias o soluciones que se pueden sugerir, enunciar o formular a ese respecto, en el contexto de aportar a una estrategia de disuasión".

Los autores.

CEEAG
CENTRO DE ESTUDIOS ESTRATÉGICOS DE LA ACADÉMIA DE GUERRA
EJÉRCITO DE CHILE

ISBN-13: 978-956-7274-08-5