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.

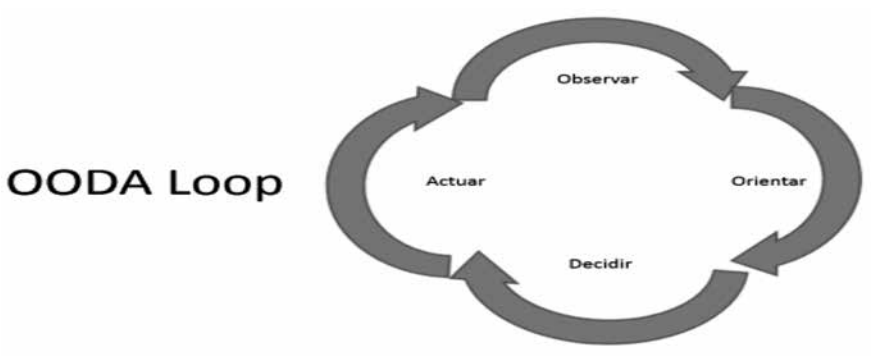
4 John Boid, The School of Advanced Airpower Studies (1997). The Paths of Heaven: The Evolution of Airpower Theory. Air University Press, Maxwell Air Force Base, Alabama, USA. p. 357.

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.

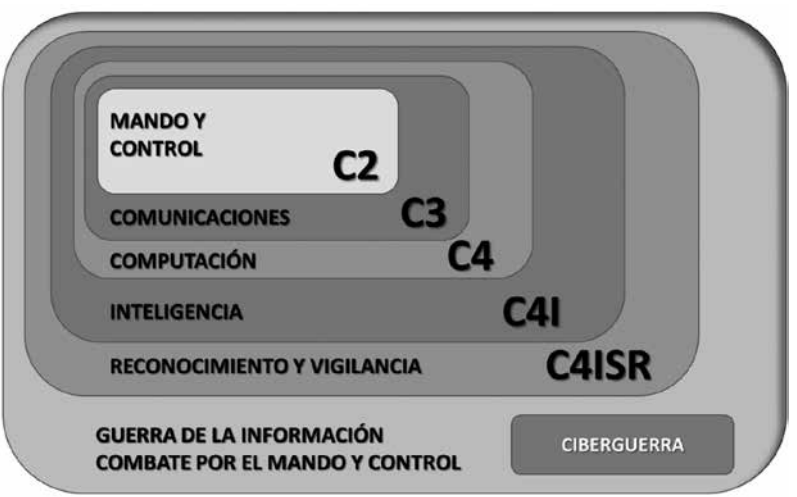
El objetivo principal de la guerra de la información (Information Warfare/ IW) es intervenir en sus fases y procesos, tanto en sus vertientes humanas como automatizadas. Para lograr su cometido IW requerirá importante apoyo de parte de la función inteligencia y de apoyo de telecomunicaciones.

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).

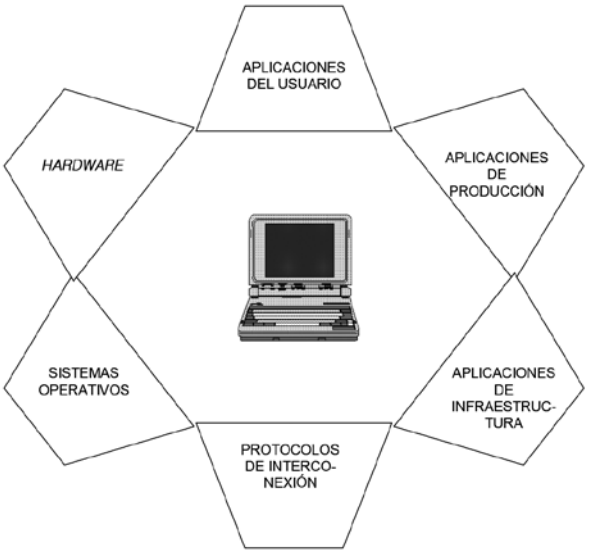
Cada uno de estos componentes se interrelacionan y conforman varios subsistemas, los que dependerán del proceso que se esté apoyando[23]:

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

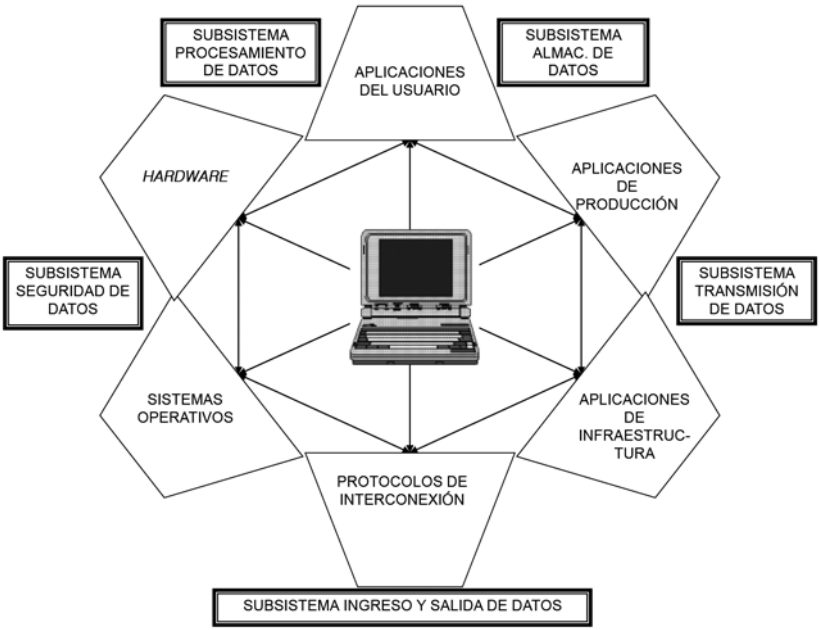
Mecanismos de *hardware*, *software* y administrativos, cuyo propósito es mantener la seguridad de datos desde el punto de vista de la integridad, confidencialidad y disponibilidad.

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

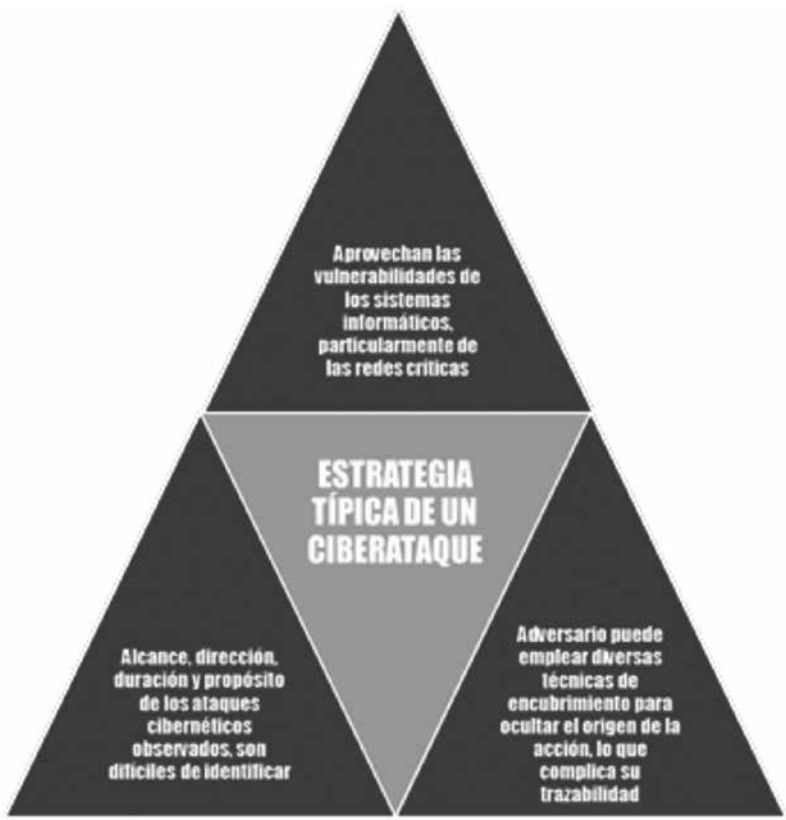
28 Rafael Calduch Cervera, *La Ocupación del Territorio Nacional y la Disuasión para su Defensa: La Cambiante Perspectiva Europea*, Universidad Complutense de Madrid.

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.